Рекомендации

Конфигурация, описанная в этом разделе, не является обязательной, но может повысить стабильность или производительность вашего развертывания.

1. Общие рекомендации

- Сразу после завершения развертывания создайте полную резервную копию и храните ее в отдельном месте. После этого регулярно создавайте резервные копии. Подробности см. в Руководстве по резервному копированию и восстановлению Менеджера управления.
- Избегайте запуска любой службы, от которой зависит развертывание (например, DNS), в качестве виртуальной машины в той же среде. Если вам необходимо запустить требуемую службу в том же развертывании, тщательно спланируйте развертывание, чтобы свести к минимуму время простоя виртуальной машины, на которой запущена требуемая служба.
- Убедитесь, что гиперконвергентные хосты обладают достаточной энтропией. Сбои могут происходить, если значение в файле **/proc/sys/kernel/random/entropy_avail** меньше 200. Чтобы увеличить энтропию, установите пакет **rng-tools**.
- Документируйте свою среду, чтобы все, кто с ней работает, знали о ее текущем состоянии и необходимых процедурах.

2. Рекомендации по безопасности

- Не отключайте никакие функции безопасности (такие как HTTPS, SELinux и брандмауэр) на хостах или виртуальных машинах.
- Создайте индивидуальные учетные записи администраторов, вместо того чтобы допускать использование одной учетной записи администратора несколькими сотрудниками. Это также полезно для отслеживания действий.
- Ограничьте доступ к хостам и создайте отдельные учетные записи. Не используйте одну учётную запись с правами `root` на всех хостах виртуализации.
- Не создавайте на хостах недоверенных пользователей.
- Избегайте установки дополнительных пакетов, таких как анализаторы, компиляторы и другие компоненты, которые повышают риск безопасности.

3. Рекомендации по хостам

- Стандартизируйте хосты в одном кластере. Это включает в себя использование одинаковых моделей оборудования и версий микропрограммного обеспечения. Смешивание различного серверного оборудования в одном кластере может привести к нестабильной производительности от хоста к хосту.
- Настройте устройства ограждения во время развертывания. Устройства ограждения необходимы для обеспечения высокой доступности.
- Используйте отдельные аппаратные коммутаторы для ограждения трафика. Если мониторинг и ограждение проходят через один коммутатор, этот коммутатор становится единой точкой отказа для обеспечения высокой доступности.
- Конфигурация хостов в гиперконвергентном кластере должна быть максимально схожей. Наиболее важно обеспечить идентичность:
  - Технологий доступа к накопителям.
  - Объемы накопителей.
  - Скорость чтения/записи накопителей.

4. Рекомендации по работе с сетью

- Объединяйте сетевые интерфейсы, особенно на продуктивных хостах. Объединение улучшает общую доступность, а также пропускную способность сети.
- Стабильная сетевая инфраструктура использующая DNS и DHCP.
- Если объединения сетевых интерфейсов (bonding) будут использоваться совместно с другим сетевым трафиком, необходимо обеспечить надлежащее качество обслуживания (QoS) для хранилища и другого сетевого трафика.
- Для оптимальной производительности и упрощения поиска и устранения неисправностей используйте виртуальные локальные сети для разделения различных типов трафика и оптимального использования сетей 10 GbE или 40 GbE.
- Если базовые коммутаторы поддерживают `jumbo frames`, установите `MTU` на максимальный размер (например, 9000), который поддерживают базовые коммутаторы. Эта настройка обеспечивает оптимальную пропускную способность, более высокую пропускную способность и меньшее использование ЦП для большинства приложений. `MTU` по умолчанию определяется минимальным размером, поддерживаемым базовыми коммутаторами. Если у вас включен `LLDP`, вы можете увидеть `MTU`, поддерживаемый хостом, в подсказках сетевой карты в окне `Установка сетей хоста`.

> Если вы измените параметры `MTU` сети, вы должны распространить эти изменения на работающие виртуальные машины в сети: "Горячее" отключение и повторное подключение **vNIC** каждой виртуальной машины, которая должна применить настройки **MTU**, или перезапуск виртуальных машин. В противном случае эти интерфейсы выйдут из строя при миграции виртуальной машины на другой хост.

- Сети 1 GbE следует использовать только для трафика управления. Используйте 10 GbE или 40 GbE для виртуальных машин и хранилищ на базе Ethernet.
- Если на хост добавляются дополнительные физические интерфейсы для использования хранилища, снимите флажок `Сеть BM`, чтобы VLAN назначалась непосредственно физическому интерфейсу.

4.1. Рекомендации по настройке сетей хоста

- Всегда используйте менеджер управления для изменения сетевой конфигурации хостов в кластерах. В противном случае вы можете создать неподдерживаемую конфигурацию.
- Если ваша сетевая инфраструктура сложная, вам может потребоваться настроить сеть хоста вручную перед добавлением хоста в среду виртуализации.
- Настроить сеть можно с помощью `Cockpit`. В качестве альтернативы можно использовать `nmtui` или `nmcli`.
- Если сеть не требуется для развертывания в режиме **Hosted Engine** или для добавления хоста в менеджер управления, настройте сеть на **Портале администрирования после добавления** хоста в менеджер управления.
- Используйте следующие соглашения об именовании:
  - Устройства VLAN: VLAN_NAME_TYPE_RAW_PLUS_VID_NO_PAD
  - Интерфейсы VLAN: physical_device.VLAN_ID (например, eth0.23, eth1.128, enp3s0.50).
  - Интерфейсы bond: bondnumber (например, bond0, bond1).
  - VLAN на объединенных интерфейсах: bondnumber.VLAN_ID (например, bond0.50, bond1.128).
- Используйте объединение сетей (bonding). `Teaming` не поддерживается в zVirt и приведет к ошибкам.
- Используйте рекомендуемые режимы объединения:
  - `Режим 0` (round-robin) - передача пакетов через сетевые интерфейсы в последовательном порядке. Пакеты передаются в цикле, который начинается с первого доступного сетевого интерфейса на хосте и заканчивается последним доступным сетевым интерфейсом на хосте. Все последующие циклы начинаются с первой доступной карты сетевого интерфейса. `Режим 0` обеспечивает отказоустойчивость и распределяет нагрузку между всеми сетевыми интерфейсными картами в связке. Обратите внимание, что `режим 0` не может

использоваться в сочетании с `bridge` и поэтому не совместим с логическими сетями виртуальных машин.

- `Режим 1` (active-backup) - переводит все сетевые интерфейсы в резервное состояние, в то время как один сетевой интерфейс остается активным. В случае отказа активного сетевого интерфейса один из резервных интерфейсов заменяет сбойный интерфейс в качестве единственного активного сетевого интерфейса в бонде. MAC-адрес соединения в `режиме 1` виден только на одном порту, чтобы предотвратить путаницу, которая может возникнуть, если MAC-адрес соединения изменится на MAC-адрес активной сетевой интерфейсной карты. `Режим 1` обеспечивает отказоустойчивость и поддерживается в zVirt.
- `Режим 2` (XOR) - выбирает сетевой интерфейс, через который будут передаваться пакеты, на основе результата операции XOR над MAC-адресами источника и назначения по модулю количества сетевых интерфейсов. Этот расчет гарантирует, что для каждого используемого MAC-адреса назначения будет выбрана одна и та же карта сетевого интерфейса. `Режим 2` обеспечивает отказоустойчивость и балансировку нагрузки и поддерживается в zVirt.
- `Режим 3` (broadcast) - передает все пакеты всем сетевым интерфейсам. `Режим 3` обеспечивает отказоустойчивость и поддерживается в zVirt.
- `Режим 4` (IEEE 802.3ad) - создает группы агрегации, в которых интерфейсы имеют одинаковые настройки скорости и дуплекса. `Режим 4` использует все сетевые интерфейсы в активной группе агрегации в соответствии со спецификацией `IEEE 802.3ad` и поддерживается в zVirt.
- `Режим 5` (adaptive transmit load balancing) - обеспечивает распределение исходящего трафика с учетом нагрузки на каждый сетевой интерфейс в связке и то, что текущий сетевой интерфейс получает весь входящий трафик. Если сетевой интерфейс, назначенный для приема трафика, выходит из строя, роль приема входящего трафика возлагается на другой сетевой интерфейс. `Режим 5` нельзя использовать в сочетании с bridge, поэтому он не совместим с логическими сетями виртуальных машин.
- `Режим 6` (adaptive load balancing) - объединяет `режим 5` (adaptive transmit load balancing) с балансировкой нагрузки при приеме для трафика IPv4 без каких-либо специальных требований к коммутатору. Для балансировки принимаемой нагрузки используется согласование ARP. `Режим 6` нельзя использовать в сочетании с `bridge`, поэтому он не совместим с логическими сетями виртуальных машин.

- Если сеть `ovirtmgmt` не используется виртуальными машинами, сеть может использовать любой поддерживаемый режим объединения.
- Если сеть `ovirtmgmt` используется виртуальными машинами, сеть должна использовать режимы объединения `1`, `2`, `3` или `4`.
- По умолчанию в zVirt используется `режим объединения 4 Dynamic Link Aggregation`. Если ваш коммутатор не поддерживает протокол `Link Aggregation`

`Control Protocol (LACP)`, используйте `режим 1 Active-Backup`.

Пример 1. Настройка VLAN на физической сетевой карте (в примере используется `nmcli`, но вы можете использовать любой инструмент)

```
nmcli connection add type vlan con-name vlan50 ifname eth0.50 dev eth0 id 50
nmcli con mod vlan50 +ipv4.dns 8.8.8.8 +ipv4.addresses 123.123.0.1/24
+ivp4.gateway 123.123.0.254
```

Пример 2. Настройка VLAN поверх бонда (в примере используется `nmcli`, но вы можете использовать любой инструмент)

```
nmcli connection add type bond con-name bond0 ifname bond0 bond.options
"mode=active-backup,miimon=100" ipv4.method disabled ipv6.method ignore
nmcli connection add type ethernet con-name eth0 ifname eth0 master bond0
slave-type bond
nmcli connection add type ethernet con-name eth1 ifname eth1 master bond0
slave-type bond
nmcli connection add type vlan con-name vlan50 ifname bond0.50 dev bond0 id
50
nmcli con mod vlan50 +ipv4.dns 8.8.8.8 +ipv4.addresses 123.123.0.1/24
+ivp4.gateway 123.123.0.254
```

Не отключайте сервис `firewalld` (межсетевой экран).

5. Рекомендации по развертыванию в архитектуре Hosted Engine

- Создайте отдельный центр данных и кластер для ВМ HostedEngine и других служб уровня инфраструктуры, если ваша инфраструктура может позволить это. Хотя виртуальная машина с менеджером управления может работать на хостах в обычном кластере, отделение от остальных виртуальных машин помогает упростить план резервного копирования и управление производительностью, доступностью и безопасностью.
- Домен хранения, предназначенный для ВМ HostedEngine, создается во время развертывания. Не используйте этот домен хранения для других виртуальных машин.
- Если ожидается большая нагрузка на хранилище, разделите сети миграции, управления и хранения, чтобы уменьшить влияние на работоспособность ВМ HostedEngine.
- Все хосты способные поддерживать работу ВМ HostedEngine должны иметь одинаковое семейство процессоров, чтобы виртуальная машина могла безопасно мигрировать

между ними. Если вы планируете создание кластера с хостами, имеющими различные семейства процессоров, необходимо начинать установку с самого раннего семейства.

- Если ВМ HostedEngine выключается или нуждается в миграции, на хосте должно быть достаточно памяти, чтобы виртуальная машина могла перезапуститься или мигрировать на него.

Создание реплицируемого тома с арбитром на виртуальной машине

В этой статье описана процедура добавления виртуальной машины-арбитра в гиперконвергентную среду zVirt.

1. Подготовка инфраструктуры

Предварительные требования:

- Развернута гиперконвергентная среда.
- В среду загружен iso-образ с установщиком zVirt Node.

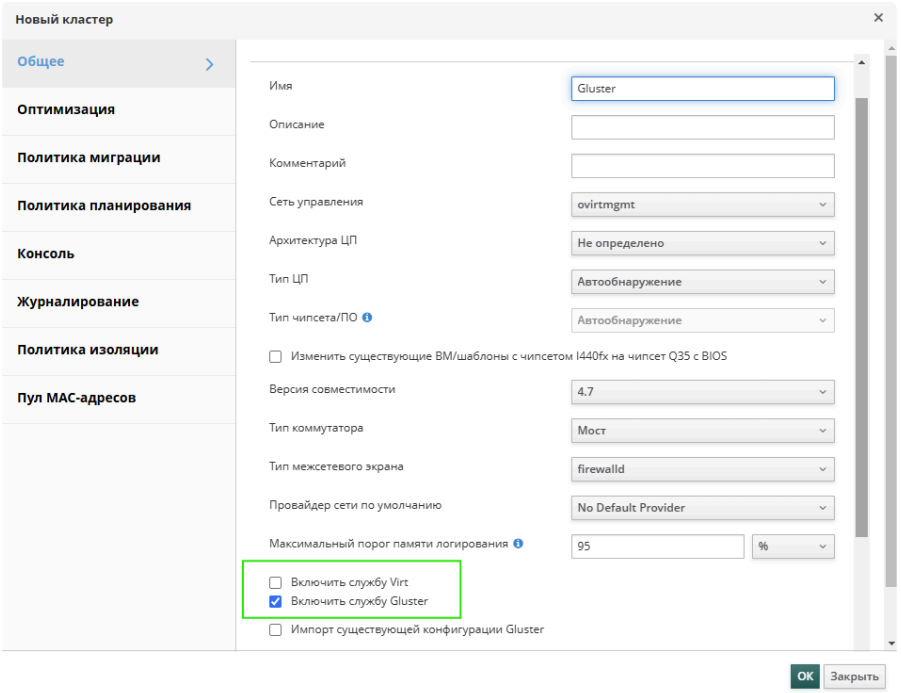
> Используйте zVirt Node той же версии, что и в развернутой среде, чтобы избежать расхождения в версиях GlusterFS.

1.1. Вариант 1. С добавлением ВМ-арбитра в среду zVirt в качестве узла Gluster

Единственное преимущество такого подхода заключается в возможности создания бриков на ВМ через портал администрирования.

Порядок действий:

1. В центре данных с гиперконвергентным кластером создайте дополнительный кластер. При создании кластера на вкладке **Общее**:
   - Архитектура ЦП: оставьте значение **Не определено**. Нужное значение позже автоматически установится на основании первого добавленного хоста.
   - Тип ЦП: оставьте значение **Автообнаружение**. Нужное значение позже автоматически установится на основании первого добавленного хоста.
   - Отключите службу **Virt**.
   - Включите службу **Gluster**



Отключение **Virt** и включение **Gluster** позволит размещать в этом кластере узлы Gluster. При этом:

1. При добавлении хостов в этот кластер не будет выполняться проверка поддержки функций виртуализации.
2. Хосты в этом кластере не смогут быть целями при миграции ВМ, что является важным требованием для арбитра.

2. В центре данных с гиперконвергентным кластером создайте логическую сеть виртуальных машин и сопоставьте её с необходимыми интерфейсами хостов в гиперконвергентном кластере.

Допустимо использовать как тегированные, так и нетегированные сети.

Эта сеть будет использоваться для взаимодействия ВМ-арбитра с другими узлами Gluster, поэтому убедитесь, что:

1. Узлы Gluster доступны из этой сети. Рекомендуется обеспечить сетевую связность с интерфейсами узлов, подключенными к сети Gluster.
2. Сеть имеет достаточную пропускную способность. Подробнее см. требования к внутренней сети в разделе Сети в системных требованиях к SDS.

3. В гиперконвергентном кластере создайте новую виртуальную машину с вычислительными ресурсами и ресурсами хранилища, соответствующими требованиям к арбитру. Подключите ВМ к сети управления (ovirtmgmt) и ранее созданной логической сети.

Настоятельно рекомендуется:

- Настроить ВМ как высокопроизводительную.
- Настроить ВМ как высокодоступную.

Без крайней необходимости не размещайте диски создаваемой ВМ в домене Gluster. Такая конфигурация может привести к тому, что при отказе домена с дисками ВМ-арбитра, также откажут все тома, для которых эта ВМ является арбитром.

4. Установите на созданную виртуальную машину zVirt Node из ранее загруженного образа.
5. После успешной установки настройте соответствующую сетевую конфигурацию на виртуальной машине.

Сетевая конфигурация должна отвечать следующим требованиям:

1. ВМ должна быть доступна для Менеджера управления по интерфейсу, подключенному к сети управления.
2. ВМ должна быть доступна для узлов Gluster по интерфейсу, подключенному к созданной ранее сети.
3. Необходимо обеспечить сетевое взаимодействие между узлами Gluster и ВМ-арбитром по FQDN. Для этого:
   - Используйте DNS-сервер. Создайте в зонах прямого и обратного просмотра соответствующие записи таким образом, чтобы все узлы Gluster, включая ВМ-арбитр успешно разрешали FQDN друг друга в прямом и обратном направлении.
   - При невозможности использования DNS-сервера, внесите соответствующие записи в файл /etc/hosts на всех узлах Gluster, включая ВМ-арбитр. Записи должны содержать корректные сопоставления IP-адресов и FQDN **ВСЕХ** узлов Gluster, в том числе ВМ-арбитра.

6. Авторизуйтесь на портале администрирования и добавьте созданную ВМ-арбитр как хост в созданный ранее кластер. Эта операция активирует на виртуальной машине службы Gluster, а также позволит управлять бриками на ВМ через портал администрирования.
7. Подключитесь по SSH к хосту, на котором при развертывании гиперконвергентной среды была настроена беспарольная аутентификация к остальным узлам Gluster. С помощью следующей команды настройте беспарольный доступ к ВМ-арбитру:

```bash
ssh-copy-id -i /root/.ssh/id_rsa.pub <arbiter-fqdn> ①
```

① Укажите FQDN, который разрешается в адрес ВМ, используемый для сети Gluster.

8. Подключите ВМ в качестве пира к кластеру Gluster:

```bash
gluster peer probe <arbiter-fqdn> ①
```

① Укажите FQDN, который разрешается в адрес ВМ, используемый для сети Gluster.

9. Проверьте статус пиров:

```bash
gluster peer status
```

Пример вывода:

```bash
Number of Peers: 3

Hostname: 10.252.11.12
Uuid: b8370eb3-827e-4fc4-8238-5c9043a2100e
State: Peer in Cluster (Connected)
Other names:
g2.vlab.local

Hostname: 10.252.11.13
Uuid: 5325d5d1-3c7a-4ae2-bae6-154e81df685c
State: Peer in Cluster (Connected)
Other names:
g3.vlab.local

Hostname: g4.vlab.local ①
Uuid: 42eb5473-58a4-4e0d-bca0-4517f61fe04c
State: Peer in Cluster (Connected) ②
```

① Добавленный узел

② Состояние `Connected`

На этом подготовка инфраструктуры завершена.

1.2. Вариант 2. Без добавления ВМ-арбитра в среду zVirt

При использовании данного варианта, брики на ВМ-арбитре необходимо создавать через CLI.

Порядок действий:

1. В центре данных с гиперконвергентным кластером создайте логическую сеть виртуальных машин и сопоставьте её с необходимыми интерфейсами хостов в гиперконвергентном кластере.

Допустимо использовать как тегированные, так и нетегированные сети.

Эта сеть будет использоваться для взаимодействия ВМ-арбитра с другими узлами Gluster, поэтому убедитесь, что:

1. Узлы Gluster доступны из этой сети. Рекомендуется обеспечить сетевую связность с интерфейсами узлов, подключенными к сети Gluster.
2. Сеть имеет достаточную пропускную способность. Подробнее см. требования к внутренней сети в разделе Сети в системных требованиях к SDS.

2. В гиперконвергентном кластере создайте новую виртуальную машину с вычислительными ресурсами и ресурсами хранилища, соответствующими требованиям к арбитру. Подключите ВМ к ранее созданной логической сети.

Настоятельно рекомендуется:

- Настроить ВМ как высокопроизводительную.
- Настроить ВМ как высокодоступную.

Без крайней необходимости не размещайте диски создаваемой ВМ в домене Gluster. Такая конфигурация может привести к тому, что при отказе домена с дисками ВМ-арбитра, также откажут все тома, для которых эта ВМ является арбитром.

3. Установите на созданную виртуальную машину zVirt Node из ранее загруженного образа.
4. После успешной установки настройте соответствующую сетевую конфигурацию на виртуальной машине.

Сетевая конфигурация должна отвечать следующим требованиям:

1. ВМ должна быть доступна для узлов Gluster по интерфейсу, подключенному к созданной ранее сети.
2. Необходимо обеспечить сетевое взаимодействие между узлами Gluster и ВМ-арбитром по FQDN. Для этого:
   - Используйте DNS-сервер. Создайте в зонах прямого и обратного просмотра соответствующие записи таким образом, чтобы все узлы Gluster, включая ВМ-арбитр успешно разрешали FQDN друг друга в прямом и обратном направлении.
   - При невозможности использования DNS-сервера, внесите соответствующие записи в файл /etc/hosts на всех узлах Gluster, включая ВМ-арбитр. Записи должны содержать корректные сопоставления IP-адресов и FQDN **ВСЕХ** узлов Gluster, в том числе ВМ-арбитра.

5. Подключитесь по SSH к хосту, на котором при развертывании гиперконвергентной среды была настроена беспарольная аутентификация к остальным узлам Gluster. С помощью следующей команды настройте беспарольный доступ к ВМ-арбитру:

```bash
ssh-copy-id -i /root/.ssh/id_rsa.pub <arbiter-fqdn> ①
```

① Укажите FQDN, который разрешается в адрес ВМ, используемый для сети Gluster.

6. Подключите ВМ в качестве пира к кластеру Gluster:

```bash
gluster peer probe <arbiter-fqdn> ①
```

① Укажите FQDN, который разрешается в адрес ВМ, используемый для сети Gluster.

7. Проверьте статус пиров:

```bash
gluster peer status
```

Пример вывода:

```bash
Number of Peers: 3

Hostname: 10.252.11.12
Uuid: b8370eb3-827e-4fc4-8238-5c9043a2100e
State: Peer in Cluster (Connected)
Other names:
g2.vlab.local

Hostname: 10.252.11.13
Uuid: 5325d5d1-3c7a-4ae2-bae6-154e81df685c
State: Peer in Cluster (Connected)
Other names:
g3.vlab.local

Hostname: g4.vlab.local ①
Uuid: 42eb5473-58a4-4e0d-bca0-4517f61fe04c
State: Peer in Cluster (Connected) ②
```

① Добавленный узел

② Состояние `Connected`

На этом подготовка инфраструктуры завершена.

2. Создание томов с бриком-арбитром на ВМ

Порядок действий:

1. На необходимых узлах Gluster, включая ВМ-арбитр, создайте брики нужного размера.

> Если при подготовке арбитра использовался вариант 1, брики можно создавать через портал администрирования.

2. Подключитесь по SSH к первому узлу Gluster (имеющему беспарольный доступ к остальным узлам).
3. Создайте реплицированный том с арбитром с помощью следующей команды:

```
gluster volume create <имя тома> replica <count> arbiter 1 host1:<brick-path>/<dir> host2:<brick-path>/<dir> host3:<arbiter-brick-path>/<dir> ① ② ③
```

① <count> - количество реплик

② <brick-path> - путь к брику на соответствующем хосте, <dir> - имя каталога для тома, который будет автоматически создан при добавлении тома.

③ Обратите внимание, что арбитр должен быть указан последним в списке

Например, для создания реплицируемого тома с 2 репликами и арбитром:

```
gluster volume create arb-vol replica 2 arbiter 1
g2.vlab.local:/gluster_bricks/brick1/arb-vol
g3.vlab.local:/gluster_bricks/brick1/arb-vol
g4.vlab.local:/gluster_bricks/arb/arb-vol
```

4. Настройте том для работы с виртуализацией:

```
gluster volume set <vol-name> group virt ①
gluster volume set <vol-name> storage.owner-gid 36 ①
gluster volume set <vol-name> storage.owner-uid 36 ①
```

① <vol-name> - имя созданного ранее тома.

5. Запустите том:

```
gluster volume start <volname>
```

6. На портале администрирования в **Хранилище** > **Тома** убедитесь, что том доступен и в состоянии **Включен**.
7. Подключите созданный том в качестве домена хранения.

Настройка параметров подключения к PostgreSQL для Менеджера управления

1. Введение

В составе zVirt используется СУБД PostgreSQL, доступ к которому настраивается при установке Менеджера в соответствии с общими рекомендациями.

При необходимости вы можете произвести дополнительную настройку параметров подключения, в соответствии с вашими требованиями.

Для этого необходимо внести изменения в файл **/var/lib/pgsql/data/pg_hba.conf**.

2. Параметры подключения

Структура файла /var/lib/pgsql/data/pg_hba.conf

```
TYPE  DATABASE  USER ADDRESS    METHOD [OPTIONS]
```

- **TYPE**: Тип подключения, может быть `local` для Unix-сокетов или `host` для TCP/IP подключений. Для TCP/IP подключений также допустимо явное указание параметров шифрования:
  - `hostssl` - использовать SSL-шифрование.
  - `hostnossl` - не использовать SSL-шифрование.
  - `hostgssenc` - использовать GSSAPI-шифрование.
  - `hostnogssenc` - не использовать GSSAPI-шифрование.
- **DATABASE**: Имя базы данных, к которой осуществляется подключение. Допустимо указание списка имен БД через запятую, а также использование ключевого слова `all`, указывающего на все БД.
- **USER**: Имя пользователя базы данных, которое будет использоваться для подключения. Допустимо указание списка имен пользователей через запятую, а также использование ключевого слова `all`, указывающего на всех пользователей.
- **ADDRESS**: Сетевой адрес или диапазон адресов, с которого разрешено подключение. Для локальных адресов используется 127.0.0.1/32 для IPv4 и ::1/128 для IPv6. Также допустимо использование имени компьютера, с которого осуществляется подключение

(должно быть разрешимо в прямом и обратном направлении), а также ключевого слова `all`, указывающего на любые адреса.

- **METHOD**: Метод аутентификации, который будет использоваться для подключения. Допустимы следующие значения:
  - `trust` - безусловное подключение. Этот метод позволяет тому, кто может подключиться к серверу с БД, войти под любым желаемым пользователем Postgres без введения пароля и без какой-либо другой аутентификации.
  - `reject` - отклонение подключения. Эта возможность полезна для «фильтрации» некоторых серверов группы, например, строка reject может отклонить попытку подключения одного компьютера, при этом следующая строка позволяет подключиться остальным компьютерам в той же сети.
  - `scram-sha-256` - подключение с парольной аутентификацией, использующей SCRAM-SHA-256.
  - `md5` - подключение с парольной аутентификацией, использующей SCRAM-SHA-256 или MD5.
  - `password` - подключение с парольной аутентификацией с открытым паролем.
  - `gss` - подключение с аутентификацией с использованием GSSAPI. Доступен только для TCP/IP подключений.
  - `ident` - получает имя пользователя операционной системы клиента, связываясь с сервером Ident, и проверяет, соответствует ли оно имени пользователя базы данных. Аутентификация ident может использоваться только для подключений по TCP/IP.
  - `peer` - получает имя пользователя операционной системы клиента из операционной системы и проверяет, соответствует ли оно имени пользователя запрашиваемой базы данных. Доступно только для локальных подключений.
  - `ldap` - аутентификация с использованием LDAP.
  - `radius` - аутентификация с использованием RADIUS.
  - `cert` - аутентификация с использованием SSL-сертификата.
- **OPTIONS**: необязательное поле, которое может содержать параметры метода аутентификации в формате `ключ=значение`.

3. Обеспечение дополнительной безопасности

Для обеспечения дополнительной безопасности подключения к базе данных PostgreSQL, используемой Менеджером управления и его компонентами, необходимо правильно настроить файл **/var/lib/pgsql/data/pg_hba.conf**.

Приведенный ниже список параметров допустимо использовать только при размещении Менеджера управления, его БД (engine) и БД хранилища данных (ovirt_engine_history) на одной машине.

В случае раздельного размещения Менеджера управления и Grafana/DWH необходимо актуализировать параметры подключения.

```
local     all                    all
peer ①
host      ovirt_engine_history   ovirt_engine_history_grafana   127.0.0.1/32
md5 ②
host      ovirt_engine_history   ovirt_engine_history_grafana   ::1/128
md5 ③
host      ovirt_engine_history   ovirt_engine_history           127.0.0.1/32
md5 ④
host      ovirt_engine_history   ovirt_engine_history           ::1/128
md5 ⑤
host      engine                 engine                         127.0.0.1/32
md5 ⑥
host      engine                 engine                         ::1/128
md5 ⑦
```

① Разрешено локальное подключение по UNIX-сокетам всем пользователям ко всем БД. Необходимо для интерактивного взаимодействия с СУБД

② Подключение Grafana к БД хранилища данных с использованием loopback IPv4 адреса. Необходимо для работы Grafana.

③ Подключение Grafana к БД хранилища данных с использованием loopback IPv6 адреса. Необходимо для работы Grafana.

④ Подключение к БД хранилища данных с использованием loopback IPv4 адреса. Необходимо для работы DWH.

⑤ Подключение к БД хранилища данных с использованием loopback IPv6 адреса. Необходимо для работы DWH.

⑥ Подключение к БД Менеджера управления с использованием loopback IPv4 адреса. Необходимо для работы служб, взаимодействующих с базой данных **engine**, в .т.ч веб порталов и утилиты engine-backup.

⑦ Подключение к БД Менеджера управления с использованием loopback IPv6 адреса. Необходимо для работы служб, взаимодействующих с базой данных **engine**, в .т.ч веб порталов и утилиты engine-backup.

При описанной выше конфигурации сохраняется работоспособность компонентов Менеджера управления, при этом получение доступа извне невозможно.

4. Применение изменений

Настройка файла **pg_hba.conf** является критически важным шагом для обеспечения безопасности и правильного функционирования базы данных PostgreSQL и компонентов Менеджера управления. Убедитесь, что все параметры указаны корректно и соответствуют вашей среде и требованиям безопасности.

Перед внесением изменений в файл, рекомендуем сделать его резервную копию.

Например:

```
cp /var/lib/pgsql/data/pg_hba.conf ~
```

После внесения изменений в файл **/var/lib/pgsql/data/pg_hba.conf**, необходимо применения новую конфигурацию. Для этого:

1. Подключитесь по SSH к Менеджеру управления и авторизуйтесь под пользователем *root*.
2. Примените конфигурацию одним из следующих способов:

   Способ 1

   - Перезапустите службу postgresql:

     ```
     systemctl reload postgresql
     ```

   Способ 2

   - Смените пользователя на postgres:

     ```
     su - postgres
     ```

   - Примените конфигурацию

     ```
     pg_ctl reload
     ```

5. Проверка подключения

Для проверки подключения к базе данных:

Локальное подключение

1. Подключитесь по SSH к Менеджеру управления и авторизуйтесь под пользователем *root*.
2. Смените пользователя на postgres:

```
su – postgres
```

3. Выполните команду `psql`. Эта команда должна запустить интерактивную оболочку postgresql.
4. Выйдите из интерактивной оболочки командой `exit`.
5. Вернитесь в сессию *root* командой `exit`.

Работоспособность компонентов Менеджера

1. На портале администрирования авторизуйтесь пользователем с административными правами.
2. Перейдите на вкладку **События**. Проконтролируйте отсутствие системных ошибок за последний час с момента изменения конфигурации подключения к СУБД.
3. Перейдите в портал мониторинга (Grafana) и убедитесь в наличии последних данных в любом разделе.

Шифрование связи в zVirt

1. Мониторинг и управление сертификатами

1.1. Общие сведения о сертификатах

В рамках работы платформы zVirt применяются различные типы сертификатов для обеспечения безопасности соединений между компонентами системы и пользователями.

Своевременное обновление сертификатов является важным требованием для обеспечения работоспособности платформы zVirt.

Автоматическое обновление сертификатов не производится, поэтому очень важно обновлять сертификаты вручную до истечения сроков их действия.

Если вы допустите истечение срока действия сертификатов, то это приведет к следующим проблемам:

- Менеджер управления и хосты перестанут взаимодействовать.
- Станет невозможным вход в веб-порталы (портал администрирования и пользовательский портал).
- Виртуальные машины продолжат работать, но управление ими будет недоступно.
- Миграция виртуальных машин станет невозможной.
- Выключение виртуальных машин приведет к невозможности их запуска.

Ниже представлена таблица с описанием основных сертификатов, используемых в zVirt.

Таблица 1. Основные сертификаты

Наименование	Назначение	Расположение
Сертификаты Менеджера управления Эти сертификаты можно найти в указанном каталоге на Менеджере управления.		
Apache-ca	Доверенный корневой сертификат Apache. По умолчанию такой же как CA.	**/etc/pki/ovirt-engine/apache-ca.pem**

Наименование	Назначение	Расположение
Apache	Используется для HTTPS соединений с веб-интерфейсом	**/etc/pki/ovirt-engine/certs/apache.cer**
websocket-proxy	Сертификат для обеспечения безопасного соединения через WebSocket, используемого для реализации двустороннего соединения между клиентом и сервером. Используется при NoVNC доступе к консоли ВМ.	**/etc/pki/ovirt-engine/certs/websocket-proxy.cer**
CA	Корневой сертификат Менеджера управления. Используется для подписи других сертификатов в системе.	**/etc/pki/ovirt-engine/ca.pem**
Engine	Используется менеджером управления для ssh и ssl аутентификации на хостах и vdsm, также используется для шифрования полей базы данных.	**/etc/pki/ovirt-engine/certs/engine.cer**
Qemu-ca	Корневой сертификат для QEMU/KVM.	**/etc/pki/ovirt-engine/qemu-ca.pem**
jboss	Сертификат сервера приложений JBoss/WildFly	**/etc/pki/ovirt-engine/certs/jboss.cer**
ovn-sdb	Сертификаты для баз данных OVN	**/etc/pki/ovirt-engine/certs/ovn-sdb.cer**
ovn-ndb		**/etc/pki/ovirt-engine/certs/ovn-ndb.cer**
vmconsole-proxy-helper	Сертификаты для создания защищённого канала связи при доступе к консоли виртуальных машин (VNC или SPICE).	**/etc/pki/ovirt-engine/certs/vmconsole-proxy-helper.cer**
vmconsole-proxy-host		**/etc/pki/ovirt-engine/certs/vmconsole-proxy-host.cer**
vmconsole-proxy-user		**/etc/pki/ovirt-engine/certs/vmconsole-proxy-user.cer**

Наименование	Назначение	Расположение
ovirt-provider-ovn	Сертификат для OVN (Open Virtual Network), инструмента для программного определения сетей виртуальных машин	**/etc/pki/ovirt-engine/certs/ovirt-provider-ovn.cer**
Сертификаты хостов		
cacert	Доверенный корневой сертификат Менеджера управления.	**/etc/pki/vdsm/certs/cacert.pem**
vdsmcert	Сертификат VDSM	**/etc/pki/vdsm/certs/vdsmcert.pem**
ca-cert (libvirt-spice)	Корневой сертификат для SPICE. Такой же как корневой сертификат VDSM (**cacert**).	**/etc/pki/vdsm/libvirt-spice/ca-cert.pem**
ca-cert (libvirt-vnc)	Корневой сертификат для VNC. Такой же как корневой сертификат VDSM (**cacert**).	**/etc/pki/vdsm/libvirt-vnc/ca-cert.pem**
ca-cert (libvirt-migrate)	Корневой сертификат, необходимый для миграции. Такой же как корневой сертификат VDSM (**cacert**).	**/etc/pki/vdsm/libvirt-migrate/ca-cert.pem**
server-cert (libvirt-spice)	Сертификат SPICE-сервера. Такой же как сертификат VDSM (**vdsmcert**).	**/etc/pki/vdsm/libvirt-spice/server-cert.pem**
server-cert (libvirt-vnc)	Сертификат VNC-сервера. Такой же как сертификат VDSM (**vdsmcert**).	**/etc/pki/vdsm/libvirt-vnc/server-cert.pem**
server-cert (libvirt-migrate)	Используется при миграции ВМ для взаимной аутентификации между хостами. Такой же как сертификат VDSM (**vdsm-cert**).	**/etc/pki/vdsm/libvirt-migrate/server-cert.pem**
clientcert	Сертификат libvirt. Такой же как сертификат VDSM (**vdsmcert**).	**/etc/pki/libvirt/clientcert.pem**

1.2. Основные каналы взаимодействия

Инфраструктура открытых ключей (PKI) используется для безопасного взаимодействия между различными компонентами платформы. Основные направления взаимодействия и способы их защиты:

Менеджер управления → SSL → vdsm

Во время развертывания хоста в качестве гипервизора сертификат регистрируется с помощью внутреннего ЦС Менеджера. Связь между Менеджером и хостом осуществляется с помощью взаимно аутентифицированной SSL-сессии на основе сертификата Менеджера (Engine) и сертификата vdsm (vdsmcert).

- Vdsm не выполняет проверку отзыва сертификата.
- На текущий момент не поддерживаются промежуточные сертификаты.

Менеджер управления → SSH → хосты

Менеджер управления способен аутентифицироваться с помощью открытого ключа своего сертификата на хостах с использованием протокола SSH.

- Менеджер не выполняет проверку отзыва сертификата.
- На текущий момент не поддерживаются промежуточные сертификаты.

Менеджер управления → SSL → база данных

В зависимости от настроек подключения, соединение с базой данных может использовать SSL. При этом доверенными являются центры сертификации jre по адресу $JAVA_HOME/lib/security/cacerts.

Пользователь → SSL → Apache → AJP → Менеджер управления

Пользователь получает доступ к Менеджеру через веб-сервер apache с помощью веб-браузера, используя TLS/SSL. По умолчанию сертификат выдается внутренним центром сертификации Менеджера, но этот сертификат может быть заменен на любой сторонний сертификат без ограничения функциональности.

Замена сертификата может быть произведена с помощью ручной настройки mod_ssl или путем замены следующих файлов в **/etc/pki/ovirt-engine**:

- apache-ca.pem
- keys/apache.p12
- keys/apache.key.nopass
- certs/apache.cer

Пользователь → SSL → SPICE

Qemu настроен на использование того же сертификата, что и vdsm. Во время инициации сессии внутренний сертификат Менеджера управления отправляется клиенту spice в

качестве доверенного корневого, чтобы сессия могла быть установлена.

> На текущий момент не поддерживаются промежуточные сертификаты.

libvirt → SSL → libvirt или qemu → SSL → qemu

Используется при миграции для взаимной аутентификации с помощью сертификата vdsm.

> На текущий момент не поддерживаются промежуточные сертификаты.

Хост → SSL → Менеджер управления

Используется для протокола регистрации, веб-сертификат извлекается при SSL-рукопожатии, на основании отпечатка устанавливается доверие. Затем извлекается открытый ключ SSH (открытый ключ сертификата Менеджера) и устанавливается для пользователя **root**.

> - Хост не выполняет проверку отзыва сертификата.

log-collector → SSH → Хосты

Использует тот же метод и ключи, что и Менеджер управления, для доступа к хостам.

1.3. Срок жизни сертификатов

В zVirt 3.3 и старше срок жизни всех самоподписанных сертификатов составляет 389 дней.

В zVirt 4.0 и новее:

- Корневые сертификаты центра сертификации Менеджера управления - 10 лет.
- Самоподписанные сертификаты, используемые для взаимодействия между Менеджером управления и хостами имеют срок жизни по умолчанию 5 лет.
- Самоподписанные сертификаты, видимые для браузеров, имеют срок жизни по умолчанию 389 дней и их необходимо обновлять раз в год. К таким сертификатам относятся сертификаты веб-портала:
  - Apache
  - Websocket-proxy

1.4. Управление сертификатами через портал администрирования

Начиная с zVirt 4.3 в портал администрирования добавлена утилита для мониторинга и управления сертификатами.

Утилита позволяет:

- Отслеживать статус сертификатов менеджера управления, веб-портала и хостов.
- Продлевать срок действия сертификатов веб-портала (Apache и Websocket-proxy).
- Выполнять замену сертификатов веб-портала (Apache и Websocket-proxy).

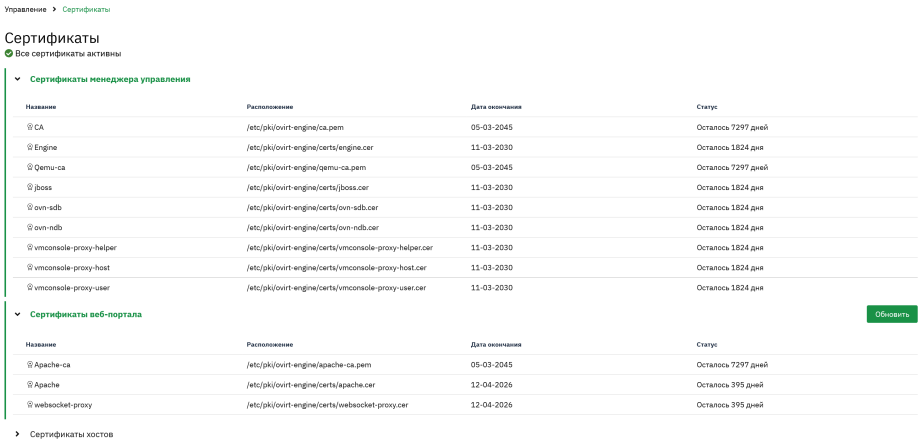
1.4.1. Мониторинг сертификатов

Для проверки текущего статуса сертификатов выполните следующие действия:

1. Авторизуйтесь на портале администрирования с правами, достаточными для управления сертификатами.
2. Перейдите в **Управление > Сертификаты**.
3. На странице сертификатов будет представлен общий статус сертификатов, а также список категорий сертификатов.

В каждой категории представлена таблица со следующими данными о сертификатах:

- Название.
- Расположение.
- Дата окончания.
- Текущий статус.



Каждый сертификат может принимать различные статусы, указывающие на возможные проблемы с сертификатом:

- В штатном состоянии в поле **Статус** указывается количество дней до окончания срока действия сертификата.
- В случае, если путь к файлу сертификата не может быть найден, то в поле **Расположение** выводится **Неизвестное расположение сертификата**.
- В случае, если не удается проверить срок действия сертификата, статус меняется на **Неизвестно**.

- Если срок действия сертификата становится 30 дней и менее, он выделяется желтым.
- Если срок действия сертификата истек, он выделяется красным.

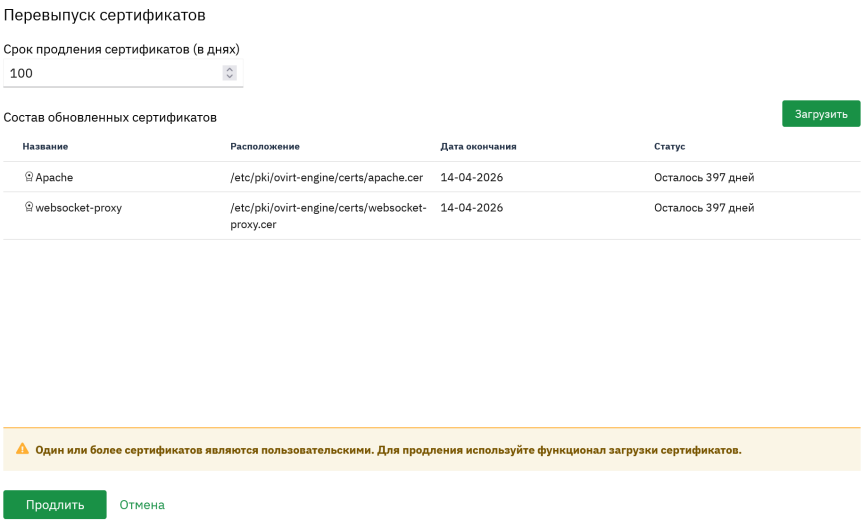
1.4.2. Обновление самоподписанных сертификатов веб-портала

Процедура обновления сертификатов применяется к сертификатам веб-портала (кроме корневого) и позволяет продлить срок их действия.

При обновлении сертификатов будут перезапущены веб-службы Менеджера управления, поэтому в течение некоторого времени будет отсутствовать доступ к веб-порталу. Это никак не влияет на работу виртуальных машин и сервисов в гостевых операционных системах.

Порядок действий:

1. Авторизуйтесь на портале администрирования с правами, достаточными для управления сертификатами.
2. Перейдите в **Управление** > **Сертификаты**.
3. Разверните категорию **Сертификаты веб-портала**.
4. Нажмите **[Обновить]**.
5. В окне перевыпуска сертификатов в поле **Срок продления сертификатов** укажите количество дней на сколько необходимо продлить сертификаты.



6. Нажмите **[Продлить]**.

Поскольку в процессе обновления сертификатов перезапускаются веб-службы менеджера, может показаться, что веб-интерфейс не среагировал на нажатие кнопки **[Продлить]**. Фактически процедура запущена, но для получения доступа к порталу необходимо обновить страницу и повторно пройти процедуру авторизации.

7. После повторной авторизации убедитесь, что в **Управление** > **Сертификаты** отображаются обновленные статусы сертификатов веб-портала.

1.4.3. Загрузка и обновление сторонних сертификатов веб-портала

Процедура загрузки и обновления сторонних сертификатов применяется к сертификатам веб-портала (кроме корневого) и позволяет продлить срок их действия.

При обновлении сертификатов будут перезапущены веб-службы Менеджера управления, поэтому в течение некоторого времени будет отсутствовать доступ к веб-порталу. Это никак не влияет на работу виртуальных машин и сервисов в гостевых операционных системах.

Предварительные требования:

- Наличие сертификата веб-портала полученного от центра сертификации в формате PKCS#12.

  Сертификат веб-портала обязательно должен иметь заполненное поле SAN со значением, дублирующим значение CN.

- Наличие корневого сертификата центра сертификации в кодировке BASE-64.

Если сертификат веб-портала подписан промежуточным сертификатом предприятия, то нужно скомпоновать единый PEM-файл, где сначала указывается промежуточный сертификат, а после него корневой сертификат.

```
-----BEGIN CERTIFICATE-----
Промежуточный сертификат
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Корневой сертификат
-----END CERTIFICATE-----
```

У промежуточного сертификата необходимо наличие секции CA: TRUE в x509 расширении.

- Файл с расширением **pfx** должен содержать внутри себя закрытый ключ для дальнейшей успешной конвертации.
- Файл с расширением **pfx** , содержащий внутри себя закрытый ключ, может быть переименован в файл с расширением p12 без дополнительной конвертации.
- Файл с расширением **pem** должен быть в кодировке BASE-64 . Проверить корректность кодировки BASE-64 можно открыв данный сертификат блокнотом. Если кодировка корректна, то сертификат будет расположен между строками -----BEGIN CERTIFICATE----- и -----END CERTIFICATE----- . Если в файле с расширением **pem** используется кодировка DER, то произвести конвертацию в BASE-64 можно командной:

  ```
  openssl x509 -in input.cer -inform DER -out output.pem
  ```

Порядок действий:

1. Авторизуйтесь на портале администрирования с правами, достаточными для управления сертификатами.
2. Перейдите в **Управление > Сертификаты**.
3. Разверните категорию **Сертификаты веб-портала**.
4. Нажмите **[Обновить]**.
5. В окне перевыпуска сертификатов нажмите **[Загрузить]**.
6. В окне загрузки:
    - В поле **Сертификат веб-портала** загрузите сертификат веб-портала.
    - Если сертификат защищен паролем, введите необходимый **Пароль**.
    - В поле **Файл промежуточных сертификатов** загрузите корневой или объединенный сертификат центра сертификации.

7. Нажмите **[Заменить]**.
8. В окне предупреждения при необходимости активируйте опцию вывода кластера из обслуживания. Нажмите **[Продолжить]**.

> Поскольку в процессе обновления сертификатов перезапускаются веб-службы менеджера, может показаться, что веб-интерфейс не среагировал на нажатие кнопки **[Продлить]**. Фактически процедура запущена, но для получения доступа к порталу необходимо обновить страницу и повторно пройти процедуру авторизации.

9. После повторной авторизации убедитесь, что в **Управление > Сертификаты** отображаются обновленные статусы сертификатов веб-портала.

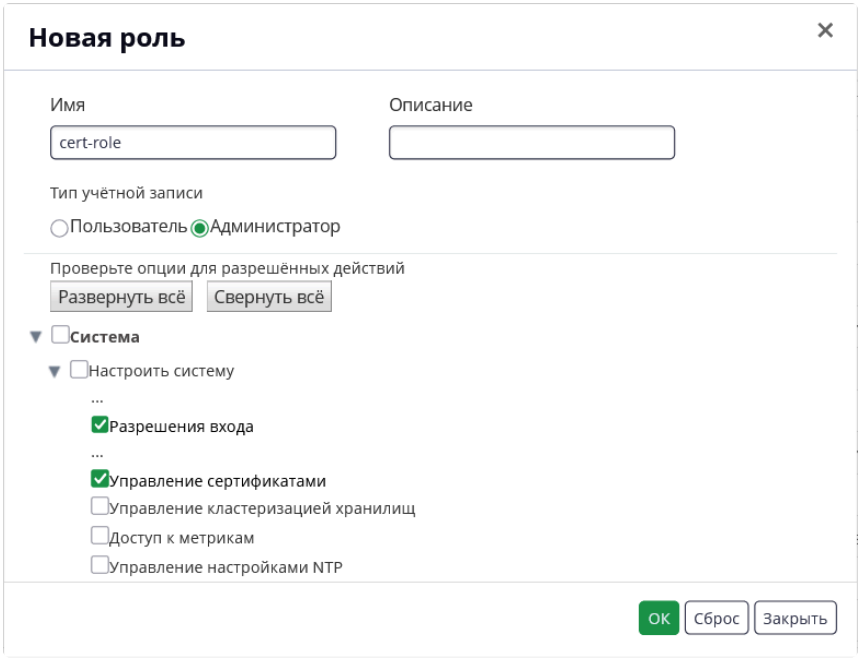
1.4.4. Настройка роли для управления сертификатами

Для настройки и управления сертификатами через портал администрирования, необходима авторизация на портале с учетной записью, имеющей системное разрешение **Управление сертификатами**.

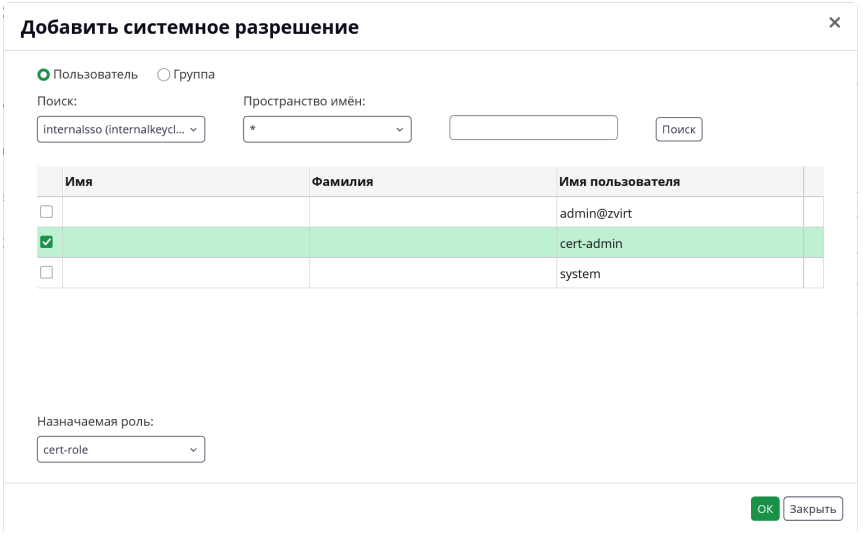
По умолчанию этим разрешением обладает любой пользователь с ролью **SuperUser**, но при необходимости можно создать новую роль с правами на управление этими сервисами.

Для этого:

1. Авторизуйтесь на портале администрирования с правами, достаточными для управления пользователями и ролями.
2. Создайте новую административную роль с разрешениями на **вход** и **Управление сертификатами**:
    a. Перейдите в **Управление** > **Настройки**.
    b. На вкладке **Роли** нажмите **[Новая]**.
    c. В окне создания роли:
        - Введите уникальное **имя** роли.
        - Выберите тип учетной записи **Администратор**.
        - В разделе опций для разрешенных действий разверните **Система** → **Настроить систему**.
        - Отметьте разрешения **Разрешения входа** и **Управление сертификатами**.
        - Нажмите **[OK]**.



3. Назначьте роль нужному пользователю или группе:
    a. В **Управление** > **Настройки**.
    b. На вкладке **Системные разрешения** нажмите **[Добавить]**.
    c. В окне добавления роли найдите нужного пользователя или группу и отметьте его
    d. В раскрывающемся списке **Назначаемая роль** выберите созданную ранее роль.



e. Нажмите **[OK]**.

4. Проверьте доступность управления сертификатами, авторизовавшись на портале администрирования пользователем с назначенной ролью.

1.5. Управление сертификатами через командную оболочку

1.5.1. Замена сертификата Менеджера управления, выданного Центром сертификации

Не изменяйте разрешения и параметры владения для каталога **/etc/pki** и его подкаталогов. Разрешение для каталога **/etc/pki** и **/etc/pki/ovirt-engine** должно оставаться в значении по умолчанию: 755.

Вы можете настроить в своей организации сертификат, выданный альтернативным Центром сертификации, чтобы идентифицировать Менеджер управления для пользователей, подключающихся через HTTPS.

Сертификат стороннего ЦС (Certificate Authority) предоставляется в виде PEM-файла. Цепочка сертификатов должна быть полной вплоть до корневого сертификата. Порядок цепочки сертификатов является критически важным, цепочка должна строится от последнего промежуточного ЦС до корневого ЦС. В противном случае при проверке подлинности сервера может произойти сбой.

Использование сертификата, выданного альтернативным Центром сертификации, для HTTPS-подключений не влияет на сертификат, используемый для аутентификации между Менеджером управления и хостами. Они будут продолжать использовать самоподписанный сертификат, созданный Менеджером управления.

1.5.1.1. Соглашения

- **/root** - расположение файлов полученных от ЦС или в процессе выполнения процедуры замены.
- **/root/apache.p12** - сертификат полученный от ЦС в формате PKCS#12.

> Для версии zVirt 4.1 файл должен быть защищен паролем `mypass`.

- **/root/ca.pem** - сертификат ЦС.
- **/root/apache.key** - новый закрытый ключ веб-сервера.
- **/root/apache.cer** - новый сертификат веб-сервера.

> - Файл с расширением **pfx** должен содержать внутри себя закрытый ключ для дальнейшей успешной конвертации.
> - Файл с расширением **pfx** , содержащий внутри себя закрытый ключ, может быть переименован в файл с расширением **p12** без дополнительной конвертации.
> - Файл с расширением **pem** должен быть в кодировке **BASE-64** . Проверить корректность кодировки **BASE-64** можно открыв данный сертификат блокнотом. Если кодировка корректна, то сертификат будет расположен между строками **-----BEGIN CERTIFICATE----- и -----END CERTIFICATE-----** . Если в файле с расширением **pem** используется кодировка **DER**, то произвести конвертацию в **BASE-64** можно командной:
>
> ```
> openssl x509 -in input.cer -inform DER -out output.pem
> ```
> BASH

1.5.1.2. Описание процедуры замены SSL-сертификата

Извлечение сертификата и закрытого ключа из пакета P12

Внутренний ЦС хранит ключ и сертификат в формате **.p12** в каталоге **/etc/pki/ovirt-engine/keys/**. Сохраните новый файл в том же месте.

1. Создайте резервную копию текущего файла **apache.p12**, например:

   ```
   cp -p /etc/pki/ovirt-engine/keys/apache.p12 /etc/pki/ovirt-engine/keys/apache.p12.bck
   ```
   BASH

2. Замените текущий файл новым, например:

   ```
   cp /root/apache.p12 /etc/pki/ovirt-engine/keys/apache.p12
   ```
   BASH

3. Извлеките закрытый ключ и сертификат.

   Если файл защищен паролем, необходимо добавить `-passin pass:<your_password>`, заменив `<your_password>` на действительный пароль.

```
openssl pkcs12 -in /etc/pki/ovirt-engine/keys/apache.p12 -nocerts -nodes >
/root/apache.key
openssl pkcs12 -in /etc/pki/ovirt-engine/keys/apache.p12 -nokeys >
/root/apache.cer
```

Замена сертификата Менеджера управления, выданного Центром Сертификации Apache

1. Если zVirt развернут в режиме Hosted Engine, необходимо перейти в консоль хоста и включить режим глобального обслуживания:

```
hosted-engine --set-maintenance --mode=global
```

2. Если сертификат **apache.p12** подписан промежуточным сертификатом предприятия, то нужно подготовить файл для добавления в хранилище сертификатов: нужно скомпоновать единый файл **ca.pem**, где сначала указывается промежуточный сертификат, а после него корневой сертификат.

```
-----BEGIN CERTIFICATE-----
Промежуточный сертификат
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Корневой сертификат
-----END CERTIFICATE-----
```

3. Добавьте сертификат ЦС в список доверенных сертификатов (**пароль mypass**), например:

```
keytool -import \
    -file /root/ca.pem  \
    -alias companyca \
    -keystore /etc/pki/ovirt-engine/.truststore
```

```
cp /root/ca.pem /etc/pki/ca-trust/source/anchors
```

```
update-ca-trust
```

4. Менеджер управления использует файл **/etc/pki/ovirt-engine/apache-ca.pem**, который является символической ссылкой на файл **/etc/pki/ovirt-engine/ca.pem**. Удалите символическую ссылку:

```
rm /etc/pki/ovirt-engine/apache-ca.pem
```

5. Сохраните сертификат ЦС, как файл **/etc/pki/ovirt-engine/apache-ca.pem**:

```
cp /root/ca.pem /etc/pki/ovirt-engine/apache-ca.pem
```

6. Создайте резервную копию существующего закрытого ключа и сертификата:

```
cp /etc/pki/ovirt-engine/keys/apache.key.nopass /etc/pki/ovirt-
engine/keys/apache.key.nopass.bck
cp /etc/pki/ovirt-engine/certs/apache.cer /etc/pki/ovirt-
engine/certs/apache.cer.bck
```

7. Скопируйте закрытый ключ:

```
cp /root/apache.key /etc/pki/ovirt-engine/keys/apache.key.nopass
```

8. Установите владельцем закрытого ключа пользователя *root* и задайте права доступа **0640**:

```
chown root:ovirt /etc/pki/ovirt-engine/keys/apache.key.nopass
chmod 640 /etc/pki/ovirt-engine/keys/apache.key.nopass
```

9. Скопируйте сертификат:

```
cp /root/apache.cer /etc/pki/ovirt-engine/certs/apache.cer
```

10. Установите владельцем сертификата пользователя *root* и задайте права доступа **0644**:

```
chown root:ovirt /etc/pki/ovirt-engine/certs/apache.cer
chmod 644 /etc/pki/ovirt-engine/certs/apache.cer
```

11. Перезапустите веб-сервер:

```
systemctl restart httpd.service
```

12. В конфигурационном файле **/usr/share/zvirt-engine/services/zvirt-engine-backend/zvirt-engine-backend.conf** сервиса измените параметр `SERVER_SSL_KEY_STORE_PASSWORD` (если строка отсутствует - добавьте), для которого укажите пароль от вашего сертификата **/root/apache.p12**. Если пароль не используется, то оставьте поле пустым (без кавычек: `SERVER_SSL_KEY_STORE_PASSWORD=`)

Пример 1. Пример содержимого файла /usr/share/zvirt-engine/services/zvirt-engine-backend/zvirt-engine-backend.conf

```
ENGINE_DEBUG_ADDRESS=*:8686
JBACKEND_HOME=/usr/share/java/zvirt/
SERVER_SSL_KEY_STORE_PASSWORD=apachep12pass
```

13. Перезапустите сервис **backend**.

```
systemctl restart zvirt-engine-backend.service
```

14. Скопируйте файл **/etc/ovirt-engine/ovirt-websocket-proxy.conf.d/10-setup.conf** и измените индекс в файле на значение, которое больше 10 (например, **99-setup.conf**). Добавьте следующие параметры в новый файл (если строки уже присутствуют их необходимо заменить):

```
SSL_CERTIFICATE=/etc/pki/ovirt-engine/certs/apache.cer
SSL_KEY=/etc/pki/ovirt-engine/keys/apache.key.nopass
```

15. Перезапустите службу **websocket-proxy**:

```
systemctl restart ovirt-websocket-proxy.service
```

16. Если вручную производились изменения файла **/etc/ovirt-provider-ovn/conf.d/10-setup-ovirt-provider-ovn.conf** или используется файл конфигурации более ранней версии zVirt, необходимо убедиться, что менеджер управления по-прежнему настроен на использование **/etc/pki/ovirt-engine/apache-ca.pem** в качестве сертификата.
17. Перезапустите сервис **ovirt-provider-ovn**:

```
systemctl restart ovirt-provider-ovn.service
```

18. Перезапустите сервис **ovirt-imageio**:

```
systemctl restart ovirt-imageio.service
```

19. Перезапустите сервис **ovirt-engine**:

```
systemctl restart ovirt-engine.service
```

20. Если zVirt развернут в режиме Hosted Engine, необходимо перейти в консоль хоста и выключить режим глобального обслуживания:

```
hosted-engine --set-maintenance --mode=none
```

Теперь пользователи могут подключаться к Порталу администрирования и Пользовательскому порталу, не видя предупреждения о подлинности сертификата, используемого для шифрования HTTPS-трафика.

2. Настройка шифрованной связи между Менеджером управления и LDAP-сервером

Данная статья применима только к установке с AAA-JDBC. Пример настройки безопасного соединения с LDAP для установки с Keycloak используйте процедуру, описанную в статье Настройка федерации пользователей с Active Directory через LDAPs.

Чтобы настроить шифрованную связь между Менеджером управления и LDAP-сервером, получите корневой сертификат LDAP-сервера, выданный Центром сертификации, скопируйте этот корневой сертификат в Менеджер управления и создайте сертификат, выданный Центром сертификации, в PEM-кодировке. Тип хранилища ключей может быть любым типом, поддерживаемым Java. В следующей процедуре используется формат Java KeyStore (JKS).

Дополнительные сведения о создании сертификата Центра сертификации в кодировке PEM и импорте сертификатов см. в разделе **X.509 CERTIFICATE TRUST STORE** файла README, размещенного в **/usr/share/doc/ovirt-engine-extension-aaa-ldap-version**.

Порядок действий:

1. В Менеджере управления скопируйте корневой сертификат LDAP-сервера, выданный Центром сертификации, в каталог **/tmp** и импортируйте корневой сертификат Центра сертификации с помощью `keytool`, чтобы создать сертификат Центра сертификации в кодировке PEM. Следующая команда импортирует корневой сертификат Центра сертификации в **/tmp/myrootca.pem** и создает корневой сертификат Центра сертификации в кодировке PEM **myrootca.jks** в **/etc/ovirt-engine/aaa/**. Выпишите местонахождение сертификата и пароль. Если вы используете интерактивный инструмент настройки, то это – вся информация, которая вам понадобится. Если вы настраиваете LDAP-сервер вручную, выполните оставшуюся часть процедуры, чтобы обновить файлы конфигурации.

```
$ keytool \
    -importcert \
    -noprompt \
    -trustcacerts \
    -alias _myrootca_ \
    -file _/tmp/myrootca.pem_ \
    -keystore _/etc/ovirt-engine/aaa/myrootca.jks_ \
    -storepass _password_
```

2. Обновите файл **/etc/ovirt-engine/aaa/profile1.properties**, внеся в него сведения о сертификате:

`${local:_basedir}` – это каталог, где находится файл конфигурации свойств LDAP, указывающий на каталог **/etc/ovirt-engine/aaa**. Если вы создали сертификат Центра сертификации в кодировке PEM в другом каталоге, замените `${local:_basedir}` полным путем к сертификату.

- Чтобы использовать startTLS (рекомендуется):

```
# Create keystore, import certificate chain and uncomment
pool.default.ssl.startTLS = true
pool.default.ssl.truststore.file = ${local:_basedir}/_myrootca.jks_
pool.default.ssl.truststore.password = _password_
```

- Чтобы использовать SSL:

```
# Create keystore, import certificate chain and uncomment
pool.default.serverset.single.port = 636
pool.default.ssl.enable = true
pool.default.ssl.truststore.file = ${local:_basedir}/_myrootca.jks_
pool.default.ssl.truststore.password = _password_
```

Чтобы продолжить настройку внешнего провайдера LDAP, см. раздел Настройка внешнего провайдера LDAP. Чтобы продолжить настройку LDAP и Kerberos для единого входа, см. раздел Настройка LDAP и Kerberos для единого входа.

Руководство по защите zVirt

1. Общие сведения

Любая кибератака заключается в последовательном продвижении атакующего к целевой системе, где выполняется запланированное зловредное действие. Такое продвижение состоит из цепочки шагов: от узла к узлу, от системы к системе, от периметра к ядру сети. Каждый шаг требует от атакующего усилий и оставляет следы.

Задача ИТ-специалистов — удлинить цепочку шагов и действий атакующего, заставить его использовать наиболее сложные техники, которые оставляют много признаков компрометации и требуют больше времени.

Для этого следует максимально использовать встроенные механизмы защиты информационных систем, а также избавиться от существенных недостатков конфигурации ИТ-инфраструктуры, таких как слабая парольная политика, уязвимости в коде приложений, избыточные права доступа, отсутствие актуальных обновлений, использование устаревших протоколов доступа и т.п.

2. Методология ХардкорИТ

Это подход, в основе которого лежит методология к определению путей и времени атаки хакера методом анализа ИТ-инфраструктуры. С его помощью можно быстро и эффективно оценить уровень защищенности конкретных ИТ-систем, критически важных для бизнеса.

В результате применения метода ХардкорИТ компанией Positive Technologies был сформирован набор рекомендаций по защите zVirt. Рекомендации подробно описаны в Руководстве по защите zVirt.

Профили безопасности

1. Рекомендации по настройке безопасности

Этот раздел содержит описание и способы закрытия уязвимостей zVirt Node.

1.1. Доступ, аутентификация и авторизация

1.1.1. Обеспечить включение параметра SSH IgnoreRhosts

Описание

Установка данного параметра сделает обязательным ввод пароля во время аутентификации по протоколу SSH.

Проверка

Выполните указанную ниже команду и убедитесь, что вывод получился следующим:

```bash
grep "^IgnoreRhosts" /etc/ssh/sshd_config

IgnoreRhosts yes ①
```

① Ожидаемый вывод

Исправление

Добавьте `IgnoreRhosts yes` в файл **/etc/ssh/sshd_config** и перезапустите сервис sshd. Например:

```bash
echo "IgnoreRhosts yes" >> /etc/ssh/sshd_config
systemctl restart sshd
```

1.1.2. Обеспечить использование только одобренных шифров

Описание

На основе исследования, проведенного различными организациями, было определено, что в симметричной части транспортного протокола SSH содержатся уязвимости, которые позволяют восстановить до 32 битов открытого текста из блока данных, зашифрованных методом Cipher Block Chaining (CBD). На основе результатов этого исследования были разработаны новые алгоритмы, использующие метод Counter. Эти алгоритмы не

подвержены указанным атакам, поэтому такие алгоритмы следует применять (при стандартном использовании).

Проверка

Выполните следующую команду и убедитесь, что в выводе не содержится каких-либо алгоритмов Cipher Block Chaining (-cbc):

```
BASH
grep "Ciphers" /etc/ssh/sshd_config

Ciphers aes256-ctr,aes192-ctr,aes128-ctr,aes256-gcm@openssh.com,aes128-gcm@openssh.com,chacha20-poly1305@openssh.com
```

Исправление

Отредактируйте файл **/etc/ssh/sshd_config**, оставив в нем только алгоритмы на основе метода Counter. Например:

```
BASH
Ciphers aes256-ctr,aes192-ctr,aes128-ctr
```

> В некоторых организациях требования к разрешенным шифрам могут быть строже. Следует убедиться, что используемые шифры соответствуют политике организации.

1.1.3. Обеспечить настройку SSH LogLevel на INFO

Описание

Параметр **LogLevel** определяет, будут ли регистрироваться события входа и выхода из системы.

SSH обладает несколькими уровнями журналирования с различной степенью детализации. Уровень **DEBUG** особенно не рекомендуется, кроме как для отладки обмена данными по SSH, поскольку при такой настройке предоставляется слишком много данных, среди которых трудно вычленить важную информацию, касающуюся безопасности. Уровень **INFO** — базовый уровень, на котором записываются только попытки входа и выхода пользователей SSH из системы. Во многих ситуациях, например при реагировании на инциденты, важно определить время, когда определенный пользователь был активен в системе. Запись событий выхода из системы может исключить из списка возможных нарушителей тех пользователей, которые не были подключены к системе, что позволит сузить круг подозреваемых.

Проверка

Выполните указанную ниже команду и убедитесь, что вывод получился следующим:

```bash
grep "^LogLevel" /etc/ssh/sshd_config

LogLevel INFO ①
```

① Ожидаемый вывод

Исправление

Добавьте `LogLevel INFO` (или измените существующее значение) в файл **/etc/ssh/sshd_config** и перезапустите сервис sshd. Например:

```bash
echo "LogLevel INFO" >> /etc/ssh/sshd_config
systemctl restart sshd
```

1.1.4. Обеспечить настройку безопасных разрешений на доступ к каталогу /etc/cron.d

Описание

Доступ к этому каталогу с правами на запись может позволить непривилегированным пользователям несанкционированно повысить свои привилегии. Предоставление доступа к этому каталогу с павами на чтение может указать непривилегированным пользователям способы повысить свои привилегии или обойти механизмы аудита.

Каталог **/etc/cron.d** содержит системные задания cron, запускаемые так же, как ежечасные, ежедневные, еженедельные и ежемесячные аналоги из **/etc/crontab**, но требующие более детального контроля времени запуска. Действия над файлами в данном каталоге нельзя производить при помощи команды `crontab`. Файлы редактируются системными администраторами с помощью текстового редактора. Следует ограничить доступ на чтение, запись и поиск для всех, кроме суперпользователя.

Проверка

Запустите следующую команду и убедитесь, что для UID и GID указано 0/root и отсутствуют разрешения для групп или остальных пользователей:

```bash
stat /etc/cron.d

Access: (0700/drwx------)  Uid: (0/root)   Gid: (0/root) ①
```

① Ожидаемый вывод

Исправление

Запустите следующие команды, чтобы установить разрешения и параметры владения для каталога **/etc/cron.d**:

```
chown root:root /etc/cron.d
chmod og-rwx /etc/cron.d
```

1.1.5. Обеспечить настройку безопасных разрешений на доступ к каталогу /etc/cron.daily

Описание

Доступ к этому каталогу с правами на запись может позволить непривилегированным пользователям несанкционированно повысить свои привилегии. Предоставление доступа к этому каталогу с павами на чтение может указать непривилегированным пользователям способы повысить свои привилегии или обойти механизмы аудита.

Каталог **/etc/cron.daily** содержит системные задания cron, запускаемые ежедневно. Действия над файлами в данном каталоге нельзя производить при помощи команды `crontab`. Файлы редактируются системными администраторами с помощью текстового редактора. Следует ограничить доступ на чтение, запись и поиск для всех, кроме суперпользователя.

Проверка

Запустите следующую команду и убедитесь, что для UID и GID указано 0/root и отсутствуют разрешения для групп или остальных пользователей:

```
stat /etc/cron.daily

Access: (0700/drwx------)  Uid: (0/root)   Gid: (0/root) ①
```

① Ожидаемый вывод

Исправление

Запустите следующие команды, чтобы установить разрешения и параметры владения для каталога **/etc/cron.daily**:

```
chown root:root /etc/cron.daily
chmod og-rwx /etc/cron.daily
```

1.1.6. Обеспечить настройку безопасных разрешений на доступ к каталогу /etc/cron.hourly

Описание

Доступ к этому каталогу с правами на запись может позволить непривилегированным пользователям несанкционированно повысить свои привилегии. Предоставление доступа к

этому каталогу с правами на чтение может указать непривилегированным пользователям способы повысить свои привилегии или обойти механизмы аудита.

Данный каталог содержит системные задания cron, запускаемые ежечасно. Действия над файлами в данном каталоге нельзя производить при помощи команды `crontab`. Файлы редактируются системными администраторами с помощью текстового редактора. Следует ограничить доступ на чтение, запись и поиск для всех, кроме суперпользователя.

Проверка

Запустите следующую команду и убедитесь, что для UID и GID указано 0/root и отсутствуют разрешения для групп или остальных пользователей:

```
BASH
stat /etc/cron.hourly

Access: (0700/drwx------)  Uid: (0/root)   Gid: (0/root) ①
```

① Ожидаемый вывод

Исправление

Запустите следующие команды, чтобы установить разрешения и параметры владения для каталога **/etc/cron.hourly**:

```
BASH
chown root:root /etc/cron.hourly
chmod og-rwx /etc/cron.hourly
```

1.1.7. Обеспечить настройку безопасных разрешений на доступ к каталогу /etc/cron.monthly

Описание

Доступ к этому каталогу с правами на запись может позволить непривилегированным пользователям несанкционированно повысить свои привилегии. Предоставление доступа к этому каталогу с правами на чтение может указать непривилегированным пользователям способы повысить свои привилегии или обойти механизмы аудита.

Каталог **/etc/cron.monthly** содержит системные задания cron, запускаемые ежемесячно. Действия над файлами в этом каталоге нельзя производить при помощи команды `crontab`. Файлы редактируются системными администраторами с помощью текстового редактора. Следует ограничить доступ на чтение, запись и поиск для всех, кроме суперпользователя.

Проверка

Запустите следующую команду и убедитесь, что для UID и GID указано 0/root и отсутствуют разрешения для групп или остальных пользователей:

```
stat /etc/cron.monthly

Access: (0700/drwx------)  Uid: (0/root)   Gid: (0/root) ①
```

① Ожидаемый вывод

Исправление

Запустите следующие команды, чтобы установить разрешения и параметры владения для каталога **/etc/cron.monthly**:

```
chown root:root /etc/cron.monthly
chmod og-rwx /etc/cron.monthly
```

1.1.8. Обеспечить настройку безопасных разрешений на доступ к каталогу /etc/cron.weekly

Описание

Доступ к этому каталогу с правами на запись может позволить непривилегированным пользователям несанкционированно повысить свои привилегии. Предоставление доступа к этому каталогу с правами на чтение может указать непривилегированным пользователям способы повысить свои привилегии или обойти механизмы аудита.

Каталог **/etc/cron.weekly** содержит системные задания cron, запускаемые еженедельно. Действия над файлами в данном каталоге нельзя производить при помощи команды `crontab`. Файлы редактируются системными администраторами с помощью текстового редактора. Следует ограничить доступ на чтение, запись и поиск для всех, кроме суперпользователя.

Проверка

Запустите следующую команду и убедитесь, что для UID и GID указано 0/root и отсутствуют разрешения для групп или остальных пользователей:

```
stat /etc/cron.weekly

Access: (0700/drwx------)  Uid: (0/root)   Gid: (0/root) ①
```

① Ожидаемый вывод

Исправление

Запустите следующие команды, чтобы установить разрешения и параметры владения для каталога **/etc/cron.weekly**:

```bash
chown root:root /etc/cron.weekly
chmod og-rwx /etc/cron.weekly
```

1.1.9. Обеспечить настройку безопасных разрешений на доступ к файлу /etc/crontab

Описание

Файл **/etc/crontab** используется демоном cron для управления своими заданиями. Следует удостовериться, что пользователь и группа **root** являются владельцами указанного файла и что доступ к файлу разрешен только владельцу.

Файл содержит информацию о том, какие системные задания запускаются с помощью cron. Доступ к указанному файлу с правами на запись может позволить непривилегированным пользователям повысить свои привилегии, в то время как доступ на чтение предоставит им информацию о системных заданиях, запускаемых в системе, что может способствовать получению ими несанкционированного привилегированного доступа.

Проверка

Запустите следующую команду и убедитесь, что для UID и GID указано 0/root и отсутствуют разрешения для групп или остальных пользователей:

```bash
stat /etc/crontab

Access: (0600/-rw-------)  Uid: (0/root)   Gid: (0/root) ①
```

① Ожидаемый вывод

Исправление

Запустите следующие команды, чтобы установить разрешения и параметры владения для файла **/etc/crontab**:

```bash
chown root:root /etc/crontab
chmod og-rwx /etc/crontab
```

1.1.10. Обеспечить настройку блокировки неактивных учетных записей через 30 дней или менее

Описание

Неактивные учетные записи представляют собой угрозу безопасности системы, так как для обнаружения неудачных попыток входа или прочих отклонений необходим вход пользователей в систему.

Учетные записи пользователей, которые не были активны в течение заданного периода времени, могут быть автоматически отключены. Следует блокировать неактивные учетные записи через 30 дней после истечения срока действия пароля.

Проверка

1. Выполните следующую команду и убедитесь, что для параметра **INACTIVE** установлено значение 30 или менее:

```
useradd -D | grep INACTIVE
INACTIVE=30
```

2. Убедитесь, что для всех пользователей с паролем в поле Password inactive указано не более 30 дней с момента истечения срока действия пароля:

```
egrep ^[^:]+:[^\!*] /etc/shadow | cut -d: -f1
<userlist> ①

chage --list <user>
Password inactive: <date> ②
```

① Список пользователей с установленными паролями

② Содержит дату блокировки неактивного пользователя. Должна быть не более 30 дней с момента истечения срока действия пароля

Данная конфигурация не применима для следующих пользователей:

- sanlock
- qemu
- postgres
- apache
- node
- ovirt-vmconsole
- grafana
- cockpit-ws
- cockpit-wsinstance
- ovirtimg
- openvswitch
- ovirt
- ceph
- vdsm

Исправление

Запустите следующую команду, чтобы установить допустимый период неактивности для всех новых пользователей:

```
useradd -D -f 30
```

1.1.11. Обеспечить настройку для стандартного атрибута umask значения 027 или более строгого

Описание

Безопасное значение по умолчанию для **umask** гарантирует, что пользователи сделали осознанный выбор относительно разрешений для своих файлов. Если для **umask** установлено стандартное значение `077`, то файлы и каталоги доступны для чтения только создателю. Значение **umask** `027` позволяет давать доступ на чтение файлов и каталогов для пользователей своей Unix-группы, значение **umask** `022` — для всех пользователей системы.

Проверка

Выполните следующие команды и убедитесь, что во всех строках, содержащих umask, указано значение 027 или более строгое:

```
grep "^umask" /etc/bashrc
umask 027 ①

grep "^umask" /etc/profile
umask 027 ①
```

① Ожидаемые значения

Исправление

В файлах **/etc/bashrc** и **/etc/profile** (а также в соответствующих файлах других оболочек, поддерживаемых системой) добавьте или отредактируйте параметры **umask** следующим образом:

```
umask 027
```

1.1.12. Обеспечить настройку параметра SSH LoginGraceTime на одну минуту или менее

Описание

Настройка небольшого значения для параметра **LoginGraceTime** минимизирует риск успешной атаки подбора паролей на сервер SSH, а также ограничивает число

одновременных не прошедших аутентификацию соединений. Хотя рекомендуемая настройка — 60 секунд (1 минута), параметр следует настраивать на основе политики организации.

Проверка

Выполните следующую команду и убедитесь, что для LoginGraceTime установлено значение не более 60:

```
grep "^LoginGraceTime" /etc/ssh/sshd_config

LoginGraceTime 60 ①
```

① Ожидаемый вывод

Исправление

Добавьте `LoginGraceTime 60` (или меньшее значение) в файл **/etc/ssh/sshd_config** и перезапустите сервис sshd. Например:

```
echo "LoginGraceTime 60" >> /etc/ssh/sshd_config
systemctl restart sshd
```

1.1.13. Обеспечить настройку предупреждающего баннера SSH

Описание

Параметр **Banner** определяет файл, чье содержимое должно быть отправлено удаленному пользователю перед получением разрешения на аутентификацию. По умолчанию баннер не отображается.

Баннеры используются для предупреждения подключающихся пользователей об определенной политике подключения. Демонстрация предупреждающего сообщения перед входом обычного пользователя в систему может в дальнейшем способствовать преследованию нарушителей, вторгшихся в компьютерную систему.

Проверка

Выполните следующую команду и убедитесь, что для Banner установлено значение `/etc/issue.net` :

```
grep "^Banner" /etc/ssh/sshd_config

Banner /etc/issue.net ①
```

① Ожидаемый вывод

Исправление

Добавьте `Banner /etc/issue.net` в файл **/etc/ssh/sshd_config** и перезапустите сервис sshd. Например:

```bash
echo "Banner /etc/issue.net" >> /etc/ssh/sshd_config
systemctl restart sshd
```

1.1.14. Обеспечить настройку времени приостановки неактивной сессии SSH

Описание

Отсутствие значения для времени приостановки соединения может позволить одному пользователю получить доступ к SSH-сессии другого пользователя (например, если пользователь отойдет от компьютера, не заблокировав экран). Настройка времени приостановки неактивной сессии как минимум уменьшает риск подобного нарушения.

Таймаут SSH-сессий управляется двумя параметрами: **ClientAliveInterval** и **ClientAliveCountMax**. При настроенном параметре **ClientAliveInterval** SSH-сессии, которые были неактивными в течение определенного времени, прерываются. При настроенном параметре **ClientAliveCountMax** служба sshd будет отправлять сообщения об активном состоянии пользователя каждый промежуток времени, заданный с помощью **ClientAliveInterval**. Когда установленное количество последовательных сообщений об активности клиента остаются без ответа от клиента, SSH-сессия прерывается. Например, если **ClientAliveInterval** настроен на 15 секунд, а **ClientAliveCountMax** — на 3, клиентская SSH-сессия будет прерываться после 45 секунд бездействия пользователя.

Хотя рекомендуемое значение **ClientAliveInterval** — 300 секунд (5 минут), следует настроить параметр согласно политике организации. Рекомендуемое значение для параметра **ClientAliveCountMax** — 0. При настройке рекомендуемого значения клиентская сессия будет прерываться после 5 минут бездействия и сообщения keepalive не будут отправляться.

Проверка

Выполните следующие команды и убедитесь, что для параметра **ClientAliveInterval** установлено значение 300 или менее, а для **ClientAliveCountMax** — 3 или менее:

```bash
grep "^ClientAliveInterval" /etc/ssh/sshd_config
ClientAliveInterval 300 ①

grep "^ClientAliveCountMax" /etc/ssh/sshd_config
ClientAliveCountMax 0 ①
```

① Ожидаемый вывод

Исправление

Добавьте `ClientAliveInterval 300` и `ClientAliveCountMax 0` в файл **/etc/ssh/sshd_-config** и перезапустите сервис sshd. Например:

```
BASH
echo "ClientAliveInterval 300" >> /etc/ssh/sshd_config
echo "ClientAliveCountMax 0" >> /etc/ssh/sshd_config
systemctl restart sshd
```

1.1.15. Обеспечить ограничение доступа к команде su

Описание

Ограничение доступа к команде `su` и использование вместо нее `sudo` позволяет более эффективно контролировать повышение пользовательских привилегий для исполнения привилегированных команд. Утилита `sudo` также предоставляет более совершенные механизмы журналирования и аудита, поскольку она способна регистрировать все команды, выполненные с помощью `sudo`, в то время как `su` фиксирует только сам факт использования программы пользователем.

Команда `su` позволяет пользователю запускать команду либо оболочку от имени другого пользователя. На замену ей была разработана программа `sudo`, которая обладает более детализированной системой контроля привилегированного доступа. Обычно команду `su` может запустить любой пользователь. Снятие комментария со строки `pam_wheel.so` в **/etc/pam.d/su** позволит ограничить использование `su` исключительно пользователями группы **wheel**.

Проверка

1. Выполните указанную ниже команду и убедитесь, что в выводе присутствует соответствующая строка:

   ```
   BASH
   grep pam_wheel.so /etc/pam.d/su
   auth required pam_wheel.so use_uid ①
   ```

   ① Ожидаемый вывод

2. Выполните следующую команду, чтобы убедиться, что состав пользователей в группе **wheel** соответствует политике организации:

   ```
   BASH
   grep wheel /etc/group
   wheel:x:10:<userlist> ①
   ```

   ① В выводе корректный список пользователей, входящих в группу **wheel**

Исправление

1. Добавьте или раскомментируйте `auth required pam_wheel.so use_uid` в файл **/etc/pam.d/su**. Например:

```bash
echo "auth required pam_wheel.so use_uid" >> /etc/pam.d/su
```

2. Добавьте необходимых пользователей в группу **wheel**:

```bash
usermod -aG wheel <user>
```

1.1.16. Обеспечить ограничение доступа по протоколу SSH

Описание

Ограничение пользовательского доступа по SSH поможет предотвратить несанкционированный доступ к системе.

Ограничить доступ к системе по SSH для пользователей и групп можно с помощью нескольких параметров. Следует воспользоваться хотя бы одним из них:

AllowUsers

Переменная `AllowUsers` позволяет системному администратору предоставлять доступ к системе по SSH определенным пользователям. Список формируется из имен пользователей, разделенных запятыми. Для этой переменной цифровые пользовательские идентификаторы не применяются. Если требуется сделать ограничение более строгим, позволив разрешенным пользователям входить в систему с определенного узла, то запись следует добавлять в формате "пользователь@узел".

AllowGroups

Переменная `AllowGroups` позволяет системному администратору предоставлять доступ к системе по SSH определенным группам пользователей. Список формируется из имен групп, разделенных запятыми. Для этой переменной цифровые идентификаторы групп не применяются.

DenyUsers

Переменная `DenyUsers` позволяет системному администратору запрещать доступ к системе по SSH определенным пользователям. Список формируется из имен пользователей, разделенных запятыми. Для этой переменной цифровые пользовательские идентификаторы не применяются. Если требуется сделать ограничение более строгим, запретив пользователям входить в систему с определенного узла, то запись следует добавлять в формате "пользователь@узел".

DenyGroups

Переменная `DenyGroups` позволяет системному администратору запрещать доступ к системе по SSH определенным группам пользователей. Список формируется из имен групп, разделенных запятыми. Для этой переменной цифровые идентификаторы групп не применяются.

Проверка

Выполните следующие команды и убедитесь, что как минимум одна из них имеет указанный вывод:

```
sshd -T | grep allowusers
AllowUsers <userlist> (1)

sshd -T | grep allowgroups
AllowGroups <grouplist> (1)

sshd -T | grep denyusers
DenyUsers <userlist> (1)

sshd -T | grep denygroups
DenyGroups <grouplist> (1)
```

(1) Ожидается наличие хотя бы одного параметра с указанием списка соответствующих пользователей или групп

Исправление

В файле **/etc/ssh/sshd_config** настройте один или несколько параметров следующим образом:

```
AllowUsers <userlist>
AllowGroups <grouplist>
DenyUsers <userlist>
DenyGroups <grouplist>
```

1.1.17. Обеспечить отключение параметра SSH HostbasedAuthentication

Описание

Хотя файлы **.rhosts** являются нерабочими при отключении их поддержки в **/etc/pam.conf**, запрет на их использование в SSH обеспечит дополнительный уровень защиты.

Параметр **HostbasedAuthentication** определяет, разрешена ли аутентификация с использованием доверенных узлов через пользователя **.rhosts** или **/etc/hosts.equiv** наряду с успешной аутентификацией клиентского узла по открытому ключу. Параметр применим только к протоколу SSH версии 2.

Проверка

Выполните указанную ниже команду и убедитесь, что вывод получился следующим:

```
grep "^HostbasedAuthentication" /etc/ssh/sshd_config
HostbasedAuthentication no (1)
```

① Ожидаемый вывод

Исправление

Добавьте `HostbasedAuthentication no` в файл **/etc/ssh/sshd_config** и перезапустите сервис sshd. Например:

```
echo "HostbasedAuthentication no" >> /etc/ssh/sshd_config
systemctl restart sshd
```

1.1.18. Обеспечить отключение параметра SSH PermitEmptyPasswords

Описание

Параметр **PermitEmptyPasswords** определяет, разрешает ли сервер SSH вход в систему учетным записям с пустыми паролями.

Запрет доступа к удаленной оболочке для учетных записей с пустыми паролями снижает риск получения злоумышленниками неавторизованного доступа к системе.

Проверка

Выполните указанную ниже команду и убедитесь, что вывод получился следующим:

```
grep "^PermitEmptyPasswords" /etc/ssh/sshd_config
PermitEmptyPasswords no ①
```

① Ожидаемый вывод

Исправление

Добавьте `PermitEmptyPasswords no` в файл **/etc/ssh/sshd_config** и перезапустите сервис sshd. Например:

```
echo "PermitEmptyPasswords no" >> /etc/ssh/sshd_config
systemctl restart sshd
```

1.1.19. Обеспечить отключение параметра SSH PermitUserEnvironment

Описание

Параметр **PermitUserEnvironment** позволяет пользователям предоставлять переменные окружения демону SSH.

Разрешение устанавливать переменные окружения с помощью демона SSH может потенциально позволить пользователям обойти механизмы безопасности (например,

настроить путь выполнения таким образом, что с помощью SSH будут выполняться троянские программы).

Проверка

Выполните указанную ниже команду и убедитесь, что вывод получился следующим:

```
grep "^PermitUserEnvironment" /etc/ssh/sshd_config
PermitUserEnvironment no ①
```

① Ожидаемый вывод

Исправление

Добавьте `PermitUserEnvironment no` в файл **/etc/ssh/sshd_config** и перезапустите сервис sshd. Например:

```
echo "PermitUserEnvironment no" >> /etc/ssh/sshd_config
systemctl restart sshd
```

1.1.20. Обеспечить отключение перенаправления пакетов X11 по SSH

Описание

Параметр **X11Forwarding** позволяет пропускать трафик X11 по протоколу SSH для осуществления удаленного соединения с графическим приложением.

Отключите перенаправление X11, за исключением случаев производственной необходимости, когда требуется использовать приложения X11 напрямую. Существует небольшой риск того, что удаленные серверы X11 пользователей, которые осуществляют вход в систему посредством SSH с перенаправлением X11, могут быть скомпрометированы другими пользователями сервера X11. Следует обратить внимание, что даже в случае отключения перенаправления X11 пользователи могут выполнять его самостоятельно с помощью дополнительного программного обеспечения.

Проверка

Выполните указанную ниже команду и убедитесь, что вывод получился следующим:

```
grep "^X11Forwarding" /etc/ssh/sshd_config
X11Forwarding no ①
```

① Ожидаемый вывод

Исправление

Измените значение параметра **X11Forwarding** на `no` в файле **/etc/ssh/sshd_config** и перезапустите сервис sshd. Например:

```
sed -i 's/X11Forwarding yes/X11Forwarding no/g' /etc/ssh/sshd_config
systemctl restart sshd
```

1.1.21. Обеспечить предоставление разрешения на использование at/cron только авторизованным пользователям

Описание

Во многих системах только системный администратор может планировать задания cron. Использование файла **cron.allow** с целью управления доступом к заданиям cron позволяет усилить безопасность системы. Проще следить за списком разрешений на доступ, чем за запрещающим списком, поскольку легко забыть добавить в последний идентификатор недавно созданного пользователя.

Настройте **/etc/cron.allow** и **/etc/at.allow**, чтобы установить право на использование данных служб только для определенных пользователей. При отсутствии **/etc/cron.allow** или **/etc/at.allow** применяются **/etc/at.deny** и **/etc/cron.deny**. Пользователи, не перечисленные в файлах **/etc/at.deny** и **/etc/cron.deny**, могут использовать at и cron. При удалении этих файлов использовать at и cron разрешается только пользователям, перечисленным в **/etc/cron.allow** и **/etc/at.allow**. Обратите внимание, что если даже конкретный пользователь не включен в список **cron.allow**, команда `cron` также может быть выполнена от его имени. Файл **cron.allow** контролирует только доступ с правами администратора к команде `crontab` для определения графика и изменения действий cron.

Проверка

1. Выполните следующие команды и проверьте, что **/etc/cron.deny** и **/etc/at.deny** не существуют:

   ```
   stat /etc/cron.deny
   stat: cannot statx '/etc/cron.deny': No such file or directory ①

   stat /etc/at.deny
   stat: cannot statx '/etc/at.deny': No such file or directory ①
   ```

   ① Ожидаемый вывод

2. Запустите следующую команду и убедитесь, что для UID и GID указано 0/root и отсутствуют разрешения на **/etc/cron.allow** и **/etc/at.allow** у групп или остальных пользователей:

   ```
   stat /etc/cron.allow
   Access: (0600/-rw-------)  Uid: (0/root)   Gid: (0/root) ①
   ```

```
stat /etc/at.allow
Access: (0600/-rw-------)  Uid: (0/root)   Gid: (0/root) ①
```

① Ожидаемый вывод

Исправление

Выполните следующие команды, чтобы удалить списки **/etc/cron.deny** и **/etc/at.deny**, а также создать **/etc/cron.allow** and **/etc/at.allow** и установить для них безопасные разрешения и параметры владения:. Например:

```bash
rm /etc/cron.deny
rm /etc/at.deny
touch /etc/cron.allow
touch /etc/at.allow
chmod og-rwx /etc/cron.allow
chmod og-rwx /etc/at.allow
chown root:root /etc/cron.allow
chown root:root /etc/at.allow
```

1.1.22. Обеспечить установку значения не выше 4 для SSH MaxAuthTries

Описание

Установка небольшого значения для параметра **MaxAuthTries** минимизирует риск успешной атаки подбора паролей на сервер SSH.

Параметр **MaxAuthTries** определяет максимальное допустимое число попыток аутентификации в рамках одного соединения. При достижении счетчиком неудачных входов в систему половины установленного числа в файл журнала syslog будут регистрироваться сообщения об ошибках с подробными сведениями о неудачной попытке.

Хотя рекомендуемая установка — 4 попытки, параметр следует настраивать на основе политики организации.

Проверка

Выполните следующую команду и убедитесь, что для **MaxAuthTries** установлено значение не более 4:

```bash
grep "^MaxAuthTries" /etc/ssh/sshd_config
MaxAuthTries 4 ①
```

① Ожидаемый вывод

Исправление

Добавьте или измените значение параметра **MaxAuthTries** в файле **/etc/ssh/sshd_config** и перезапустите сервис sshd. Например:

```
echo "MaxAuthTries 4" >> /etc/ssh/sshd_config
systemctl restart sshd
```

1.1.23. Обеспечить установку истечения срока действия пароля на 365 дней ли менее

Описание

Параметр **PASS_MAX_DAYS** в **/etc/login.defs** позволяет администратору установить срок действия пароля. Следует настроить для этого параметра значение 365 или менее.

Срок действия паролей является ограничивающим фактором при проведении атак: злоумышленнику необходимо воспользоваться скомпрометированными учетными данными, либо скомпрометировать их путем онлайн-подбора паролей в указанные сроки. Поэтому уменьшение значения параметра усложнит задачу для потенциальных злоумышленников.

Проверка

1. Выполните следующую команду и убедитесь, что для параметра **PASS_MAX_DAYS** установлено значение 365 или менее:

   ```
   grep PASS_MAX_DAYS /etc/login.defs
   PASS_MAX_DAYS 365 ①
   ```

   ① Ожидаемый вывод

2. Убедитесь, что для всех пользователей с паролем максимальное количество дней между сменами пароля установлено на 365 или менее:

   ```
   egrep ^[^:]+:[^\!*] /etc/shadow | cut –d: –f1
   <userlist> ①

   chage ––list <user>
   Maximum number of days between password change: 365 ②
   ```

   ① Список пользователей с паролями

   ② Ожидаемый срок действия паролей 365 дней или меньше

Исправление

1. Установите значение 365 или меньше для параметра **PASS_MAX_DAYS** в **/etc/login.defs**:
2. Измените пользовательские настройки для всех пользователей с паролем таким образом, чтобы они соответствовали требованиям:

```
chage --maxdays 365 <user>
```

BASH

Данная конфигурация не применима для следующих пользователей:

- sanlock
- qemu
- postgres
- apache
- node
- ovirt-vmconsole
- grafana
- cockpit-ws
- cockpit-wsinstance
- ovirtimg
- openvswitch
- ovirt
- ceph
- vdsm

1.1.24. Обеспечить установку минимального количества дней между сменами пароля на 7 или более

Описание

Ограничение частоты смены пароля позволит администратору предотвратить многократное изменение пользователем пароля в попытке обойти запрет на его повторное использование.

Параметр **PASS_MIN_DAYS** в **/etc/login.defs** позволяет администратору ограничить возможность смены пароля определенным количеством дней. Следует настроить для этого параметра значение 7 или более.

Проверка

1. Выполните следующую команду и убедитесь, что для параметра **PASS_MIN_DAYS** установлено значение 7 или более:

```
grep PASS_MIN_DAYS /etc/login.defs
PASS_MIN_DAYS 7 ①
```

BASH

① Ожидаемый вывод

2. Убедитесь, что для всех пользователей с паролем минимальное количество дней между сменами пароля установлено на 7 или более:

```
egrep ^[^:]+:[^\!*] /etc/shadow | cut -d: -f1
<userlist> ①

chage --list <user>
Minimum number of days between password change: 7 ②
```

① Список пользователей с паролями

② Ожидаемый количество дней между сменами пароля 7 дней или более

Исправление

1. Установите значение 7 или более для параметра **PASS_MIN_DAYS** в **/etc/login.defs**:
2. Измените пользовательские настройки для всех пользователей с паролем таким образом, чтобы они соответствовали требованиям:

```
chage --mindays 7 <user>
```

Данная конфигурация не применима для следующих пользователей:

- sanlock
- qemu
- postgres
- apache
- node
- ovirt-vmconsole
- grafana
- cockpit-ws
- cockpit-wsinstance
- ovirtimg
- openvswitch
- ovirt
- ceph
- vdsm

1.1.25. Обеспечить установку протокола SSH версии 2

Описание

SSH поддерживает два разных и несовместимых протокола: SSH1 и SSH2. SSH1 является первой версией протокола со значительными проблемами в области безопасности. SSH2 является более поздней и безопасной версией.

Проверка

Выполните следующую команду и убедитесь, что для параметра **Protocol** установлено значение 2:

```
grep "^Protocol" /etc/ssh/sshd_config
Protocol 2 ①
```

BASH

① Ожидаемый вывод

Исправление

Добавьте или измените значение параметра **Protocol** в файле **/etc/ssh/sshd_config** и перезапустите сервис sshd. Например:

```
echo "Protocol 2" >> /etc/ssh/sshd_config
systemctl restart sshd
```

BASH

1.1.26. Обеспечить установку требований к созданию паролей

Описание

Надежные пароли защитят систему от взлома методом перебора паролей.

Модуль **pam_cracklib.so** определяет степень надежности пароля. Он проверяет: длину пароля, наличие в нем сочетания разных типов символов (буквы, цифры и др.), употребление словарных слов и пр. Далее приводятся описания параметров **pam_cracklib.so**:

- **try_first_pass** — извлечь пароль из предыдущего сохраненного PAM-модуля, при отсутствии такового запросить пароль у пользователя;
- **retry=3** — разрешать 3 попытки перед отправкой сообщения об ошибке;
- **minlen=14** — минимальная длина пароля должна составлять от 14 символов;
- **dcredit=-1** — в пароле должна содержаться хотя бы одна цифра;
- **ucredit=-1** — в пароле должна содержаться хотя бы одна буква верхнего регистра;
- **ocredit=-1** — в пароле должен содержаться хотя бы один символ;
- **lcredit=-1** — в пароле должна содержаться хотя бы одна буква нижнего регистра.

Модуль **pam_pwquality.so** работает аналогично, только параметры **minlen**, **dcredit**, **ucredit**, **ocredit** и **lcredit** хранятся файле **/etc/security/pwquality.conf**.

Указанные выше настройки являются примером. Измените значения в соответствии с политикой паролей организации.

Проверка

Убедитесь, что требования к созданию паролей заданы как указано ниже или более строго. Указанные параметры обычно настраиваются с помощью модулей **pam_cracklib.so** или **pam_pwquality.so**, которые находятся в **/etc/pam.d/common-password** или **/etc/pam.d/system-auth**.

Например:

```
BASH
grep '^password' /etc/pam.d/system-auth

password required pam_cracklib.so try_first_pass retry=3 minlen=14 dcredit=-1
ucredit=-1 ocredit=-1 lcredit=-1
password requisite pam_pwquality.so try_first_pass retry=3
```

Если используется **pam_pwquality.so**, следует также проверить параметры в **/etc/security/pwquality.conf**:

```
BASH
minlen=14
dcredit=-1
ucredit=-1
ocredit=-1
lcredit=-1
```

Исправление

Установите требования к созданию паролей в соответствии с политикой организации.

Отредактируйте соответствующий конфигурационный файл /etc/pam.d/, чтобы добавить или изменить строки **pam_cracklib.so** или **pam_pwquality.so** таким образом, чтобы они включали необходимые параметры. Например:

```
BASH
password required pam_cracklib.so try_first_pass retry=3 minlen=14 dcredit=-1
ucredit=-1 ocredit=-1 lcredit=-1
password requisite pam_pwquality.so try_first_pass retry=3
```

Если используется **pam_pwquality.so**, следует также установить параметры в /etc/security/pwquality.conf:

```
BASH
minlen=14
dcredit=-1
ucredit=-1
ocredit=-1
lcredit=-1
```

1.2. Журналирование и аудит

1.2.1. Запретить автоматическое удаление журналов аудита

Описание

В контекстах повышенной безопасности преимущества от хранения длительной истории аудита перевешивают возможные издержки.

Параметр **max_log_file_action** в файле **/etc/audit/auditd.conf** контролирует, каким образом обрабатывать файлы журнала аудита, достигшие максимального размера. Значение **keep_logs** обеспечит ротацию журналов и при этом исключит удаление старых журналов.

Проверка

Выполните следующую команду и убедитесь, что для параметра **Protocol** установлено значение 2:

```
BASH
grep max_log_file_action /etc/audit/auditd.conf
max_log_file_action = keep_logs ①
```

① Ожидаемый вывод

Исправление

Установите для параметра **max_log_file_action** в файле **/etc/audit/auditd.conf** значение `keep_logs` .

1.2.2. Обеспечить активное состояние службы rsyslog

Описание

Пакет **rsyslog** после установки необходимо активировать.

Если пакет **rsyslog** не активировать после установки, в системе по умолчанию может использоваться служба **syslogd** или вообще отсутствовать регистрация событий.

Проверка

Выполните следующую команду и убедитесь, что служба **rsyslog** находится в состоянии **enabled**:

```
BASH
systemctl is-enabled rsyslog
enabled ①
```

① Ожидаемый вывод

Исправление

Активируйте службу rsyslog:

```
systemctl enable --now rsyslog
```

1.2.3. Обеспечить настройку стандартных разрешений для файлов rsyslog

Описание

Следует убедиться, что файлы журналов имеют корректные права доступа, чтобы обеспечить архивацию и защиту данных, которые потенциально могут использоваться злоумышленниками для атак.

Служба **rsyslog** будет создавать файлы, которых пока не существует в системе. Следует контролировать, какие разрешения будут применяться к этим создаваемым файлам.

Необходимо убедиться, что эта настройка не переопределена менее строгими параметрами в любом файле конфигурации в каталоге **/etc/rsyslog.d/**.

Проверка

Выполните следующую команду и убедитесь, что значение `$FileCreateMode` — `0640` или более строгое:

```
grep ^\$FileCreateMode /etc/rsyslog.conf /etc/rsyslog.d/*.conf
enabled ①
```

① Ожидаемый вывод

Исправление

Отредактируйте файл **/etc/rsyslog.conf**, настроив для `$FileCreateMode` значение `0640` или более строгое. Убедитесь, что эта настройка не переопределена менее строгими параметрами в любом файле конфигурации в каталоге **/etc/rsyslog.d/**. Перезапустите службу **rsyslog**.

1.2.4. Обеспечить неизменяемость конфигурации аудита

Описание

Следует настроить аудит системы таким образом, чтобы правила аудита не могли быть изменены с помощью **auditctl**. Установка флага "-e 2" вводит аудит в неизменяемый режим. Изменения в настройках аудита могут быть произведены только после перезагрузки системы.

Проверка

Выполните следующую команду и убедитесь, что в выводе присутствует необходимый флаг:

```
grep "^\s*[^#]" /etc/audit/audit.rules | tail -1
-e 2 ①
```

① Ожидаемый вывод

Исправление

Вставьте значение `-e 2` строку в конец файла **/etc/audit/audit.rules**.

1.2.5. Обеспечить отключение системы при заполненных журналах аудита

Описание

Демон **auditd** можно настроить на выполнение остановки системы при заполнении журналов аудита.

В контекстах повышенной безопасности угроза обнаружения неавторизованного доступа либо невозможность отрицать факт получения или отправки содержимого перевешивает выгоду от доступности системы.

Проверка

Выполните указанные команды и убедитесь, что в выводе содержаться соответствующие значения:

```
grep space_left_action /etc/audit/auditd.conf
space_left_action = email ①

grep action_mail_acct /etc/audit/auditd.conf
action_mail_acct = root ①

grep admin_space_left_action /etc/audit/auditd.conf
admin_space_left_action = halt ①
```

① Ожидаемый вывод

Исправление

Настройте следующие параметры в файле **/etc/audit/auditd.conf**:

```
space_left_action = email
action_mail_acct = root
admin_space_left_action = halt
```

1.2.6. Обеспечить отправку журналов rsyslog на удаленный узел журналирования

Описание

Утилита **rsyslog** позволяет отправлять собранные ей журналы на удаленный узел журналирования, на котором запущена служба **syslogd**, или получать сообщения с удаленных узлов, тем самым сокращая объем работы для администратора.

Хранение данных регистрации событий на удаленном узле защищает целостность журналов регистрации в случае локальных атак. Если злоумышленник получит доступ суперпользователя к локальной системе, то сможет модифицировать или удалить хранящиеся в ней данные журналов.

Проверка

Проверьте файлы /etc/rsyslog.conf и /etc/rsyslog.d/*.conf и убедитесь, что журналы отправляются на централизованный узел (loghost.example.com — пример имени централизованного узла журналирования):

```
grep "^*.*[^I][^I]*@" /etc/rsyslog.conf /etc/rsyslog.d/*.conf

*.* @@loghost.example.com ①
```

① Ожидаемый вывод

Исправление

1. Отредактируйте файлы /etc/rsyslog.conf и /etc/rsyslog.d/*.conf, добавив следующую строку (loghost.example.com — пример имени централизованного узла журналирования):

   ```
   *.* @@loghost.example.com
   ```

2. Выполните следующую команду, чтобы перезагрузить конфигурацию **rsyslogd**:

   ```
   kill -HUP rsyslogd
   ```

Комбинация знаков `@@` позволяет настроить использование TCP для передачи на сервер сообщений журналов **rsyslog**, что является более надежным транспортом, чем установленный по умолчанию протокол UDP.

1.2.7. Обеспечить сбор данных о запуске сеансов

Описание

Отслеживание изменений в соответствующих файлах позволит системному администратору получать уведомления о событиях входа в систему в необычное время, что может обозначать вторжение в систему (то есть вход пользователя в систему в нехарактерное для него время).

Следует отслеживать события запуска сеанса. Необходимо задать настройки таким образом, чтобы события сеансов записывались в соответствующие файлы:

- Файл **/var/run/utmp** отслеживает всех пользователей, находящихся на данный момент в системе. Всем этим записям аудита будет присвоен идентификатор sessions.
- В файл **/var/log/wtmp** записываются события входа и выхода из системы, ее выключения и перезагрузки.
- В файле **/var/log/btmp** регистрируются неудачные попытки входа в систему, прочитать их можно при помощи команды `/usr/bin/last –f /var/log/btmp`. Всем этим записям аудита будет присвоен идентификатор logins.

Проверка

Выполните указанную ниже команду и убедитесь, что в выводе содержатся соответствующие значения:

```
BASH
grep session /etc/audit/audit.rules

–w /var/run/utmp –p wa –k session ①
–w /var/log/wtmp –p wa –k logins ①
–w /var/log/btmp –p wa –k logins ①
```

① Ожидаемый вывод

Исправление

Вставьте следующие строки в файл **/etc/audit/audit.rules**:

```
BASH
–w /var/run/utmp –p wa –k session
–w /var/log/wtmp –p wa –k logins
–w /var/log/btmp –p wa –k logins
```

1.2.8. Обеспечить сбор изменений привилегий на администрирование системы (sudoers)

Описание

Изменения в файле **/etc/sudoers** могут сигнализировать о неавторизованной модификации привилегий на администрирование системы.

Отслеживайте изменения привилегий на администрирование системы. Это возможно, если система была правильно настроена и системные администраторы сначала заходят в систему от своего имени и уже потом используют команду `sudo` для выполнения привилегированных команд. При изменении файла **/etc/sudoers** или его свойств в журнале аудита будет формироваться запись. Такие записи будут иметь идентификатор scope.

Проверка

Выполните указанную ниже команду и убедитесь, что в выводе содержатся соответствующие значения:

```
grep scope /etc/audit/audit.rules

-w /etc/sudoers -p wa -k scope ①
-w /etc/sudoers.d -p wa -k scope ①
```

BASH

① Ожидаемый вывод

Исправление

Вставьте следующие строки в файл **/etc/audit/audit.rules**:

```
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d -p wa -k scope
```

BASH

1.2.9. Обеспечить сбор неудачных попыток неавторизованного доступа к файлам

Описание

Неудачные попытки открыть, создать или усечь файлы могут сигнализировать о попытках злоумышленника получить несанкционированный доступ в систему.

Отслеживайте неудачные попытки осуществления доступа к файлам. Рассматриваемые настройки связаны с системными вызовами, управляющими созданием (creat), открытием (open, openat) и усечением (truncate, ftruncate) файлов. Запись в журнале аудита будет производиться, если пользователь не является привилегированным (auid > = 500), если речь не идет о событии демона (auid=4294967295) и если системный вызов выдал EACCES (разрешение на доступ к файлу отклонено) или EPERM (любая другая систематическая ошибка, связанная с определенным системным вызовом). Всем записям аудита присваивается идентификатор access.

Исправление

Выполните действия, указанные в разделе 4.1.11 документа CIS Distribution Independent Linux Benchmark v1.1.0.

1.2.10. Обеспечить сбор событий входа и выхода

Описание

Отслеживание событий входа в систему и выхода из нее позволяет системному администратору получить данные об атаках подбора пароля на учетные записи пользователей.

Необходимо отслеживать события входа и выхода из системы. Следует задать настройки таким образом, чтобы события входа в систему и выхода из нее записывались в соответствующие файлы:

- Файл **/var/log/faillog** записывает события неудачных попыток входа в систему.
- В файле **/var/log/lastlog** регистрируются последние успешные попытки входа пользователя.
- В файле **/var/log/tallylog** содержатся записи о неудачных попытках входа с помощью модуля pam_tally2.

Проверка

Выполните указанную ниже команду и убедитесь, что в выводе содержатся соответствующие значения:

```
grep logins /etc/audit/audit.rules

-w /var/log/faillog -p wa -k logins ①
-w /var/log/lastlog -p wa -k logins ①
-w /var/log/tallylog -p wa -k logins ①
```

① Ожидаемый вывод

Исправление

Вставьте следующие строки в файл /etc/audit/audit.rules:

```
-w /var/log/faillog -p wa -k logins
-w /var/log/lastlog -p wa -k logins
-w /var/log/tallylog -p wa -k logins
```

1.2.11. Обеспечить сбор событий загрузки и выгрузки модуля ядра

Описание

Отслеживание использования **insmod**, **rmmod** и **modprobe** поможет системным администраторам найти свидетельства загрузки и выгрузки модуля ядра неавторизованным пользователем с возможной компрометацией системы. Отслеживание системных вызовов `init_module` и `delete_module` позволит определить попытки неавторизованного пользователя воспользоваться другой программой для загрузки и выгрузки модулей.

Проверка

Выполните указанную ниже команду и убедитесь, что в выводе содержатся соответствующие значения:

Исправление

Вставьте следующие строки в файл /etc/audit/audit.rules:

1.2.12. Обеспечить сбор событий использования привилегированных команд

Описание

Выполнение привилегированных команд непривилегированными пользователями может сигнализировать о попытке злоумышленника получить несанкционированный доступ в систему.

Отслеживайте привилегированные программы (с битами setuid и/или setgid, настроенными на выполнение), чтобы определить, запущены ли программы непривилегированными пользователями.

Проверка

Выполните следующую команду, заменив `<partition>` списком разделов, из которых в вашей системе могут выполняться программы:

```
BASH
find <partition> -xdev \( -perm -4000 -o -perm -2000 \) -type f | awk '{print \
    "-a always,exit -F path=" $1 " -F perm=x -F auid>=500 -F auid!=4294967295 \
    -k privileged" }'
```

Убедитесь, что все выведенные строки находятся в файле **/etc/audit/audit.rules**.

Исправление

Чтобы соблюсти данное требование, системный администратор должен выполнить команду `find` и обнаружить все привилегированные программы. После чего требуется добавить строку аудита для каждой из них. Ниже приведены соответствующие параметры аудита:

- `-F path=" $1 "` — заполнить каждое имя файла, найденного при помощи команды **find** и обработанного **awk**;
- `-F perm=x` — сделать запись аудита, если файл выполняется;
- `-F auid>=500` — сделать запись, если команда выполняется от имени непривилегированного пользователя;
- `-F auid!= 4294967295` — игнорировать события демонов.

Всем этим записям аудита должен быть присвоен идентификатор privileged.

Выполните следующую команду, заменив `<partition>` списком разделов, из которых в вашей системе могут выполняться программы:

```
find <partition> -xdev \( -perm -4000 -o -perm -2000 \) -type f | awk '{print \
"-a always,exit -F path=" $1 " -F perm=x -F auid>=500 -F auid!=4294967295 \
-k privileged" }'
```
BASH

Добавьте все выведенные строки в файл **/etc/audit/audit.rules**.

1.2.13. Обеспечить сбор событий, связанных с изменением даты и времени

Описание

Неожиданные изменения системной даты или времени могут быть признаком осуществления вредоносных действий в системе.

Следует регистрировать события, в результате которых изменились системные дата или время. Рекомендуется настроить параметры таким образом, чтобы определить, выполнялись ли системные вызовы `adjtimex` (настройка часов ядра), `settimeofday` (установка времени при помощи структур timeval и timezone), `stime` (применение секунд с 1/1/1970) или `clock_settime` (установка нескольких внутренних часов и таймеров), и обеспечить их аудит в файл **/var/log/audit.log** при выходе с присвоением идентификатора записей "time-change".

Исправление

Выполните действия, указанные в разделе 4.1.4 документа CIS Distribution Independent Linux Benchmark v1.1.0.

1.2.14. Обеспечить сбор событий, связанных с изменением информации о пользователях или группах

Описание

Непредвиденные изменения в файлах **group**, **passwd**, **shadow** и **gshadow** либо **/etc/security/opasswd** могут быть признаком компрометации системы и попыток злоумышленника скрыть свои действия или компрометировать другие учетные записи.

Следует регистрировать события, повлиявшие на файлы **group**, **passwd** (ID пользователей), **shadow** и **qshadow** (пароли) или **/etc/security/opasswd** (старые пароли, основанные на параметре `remember` в конфигурации PAM). Необходимо задать такие настройки, чтобы отслеживать открытие файлов для редактирования или изменение их атрибутов (например, прав доступа) и присваивать этим событиям идентификатор identity в файле журнала аудита.

Проверка

Выполните указанную ниже команду и убедитесь, что в выводе присутствуют соответствующие записи:

```
grep identity /etc/audit/audit.rules

-w /etc/group -p wa -k identity ①
-w /etc/passwd -p wa -k identity ①
-w /etc/gshadow -p wa -k identity ①
-w /etc/shadow -p wa -k identity ①
-w /etc/security/opasswd -p wa -k identity ①
```

① Ожидаемый вывод

Исправление

Вставьте следующие строки в файл /etc/audit/audit.rules:

```
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
```

1.2.15. Обеспечить сбор событий, связанных с изменением прав избирательного управления доступом

Описание

Отслеживание изменений в свойствах файлов поможет системному администратору обнаружить действия, указывающие на вторжение в систему или нарушение политики безопасности

Необходимо отслеживать изменения в файловых правах на доступ, свойствах, владении и группе. Рассматриваемые ниже параметры отслеживают изменения в системных вызовах, которые влияют на права доступа и свойства файлов. Системные вызовы chmod, fchmod и fchmodat влияют на права на доступ, связанные с файлом. Вызовы `chown`, `fchown`, `fchownat` и `lchown` влияют на свойства владельца и группы файла. Вызовы `setxattr`, `lsetxattr`, `fsetxattr` (установить расширенные свойства файла) и `removexattr`, `lremovexattr`, `fremovexattr` (удалить расширенные свойства файла) управляют расширенными свойствами файла. Во всех случаях запись аудита будет производиться только для несистемных идентификаторов пользователя (`auid >= 500`) и проигнорирует события демонов (`auid = 4294967295`). Все записи аудита получат идентификатор perm_mod.

Исправление

Выполните действия, указанные в разделе 4.1.10 документа CIS Distribution Independent Linux Benchmark v1.1.0.

1.2.16. Обеспечить сбор событий, связанных с изменением сетевого окружения системы

Описание

Следует регистрировать изменения в файлах сетевого окружения или системных вызовах. Следует настроить параметры, которые отслеживают системные вызовы `sethostname` (установка имени узла) или `setdomainname` (установка имени домена) и записывают событие аудита по окончании системного вызова. Также следует настроить параметры, которые отслеживают файлы **/etc/issue** и **/etc/issue.net** (сообщения, выводимые перед входом в систему), **/etc/hosts** (файл, содержащий имена узлов и соответствующие им IP-адреса) и **/etc/sysconfig/network** (каталог со сценариями и конфигурациями сетевого интерфейса).

Исправление

Выполните действия, указанные в разделе 4.1.6 документа CIS Distribution Independent Linux Benchmark v1.1.0.

1.2.17. Обеспечить сбор событий, связанных с изменениями в политике мандатного управления доступом системы

Описание

Изменения в файлах каталога **/etc/selinux** могут сигнализировать о попытках неавторизованного пользователя модифицировать параметры управления доступом и контексты безопасности, что может привести к компрометации системы.

Проверка

Выполните следующую команду и убедитесь, что в выводе присутствуют соотвествующие значения:

```
grep MAC-policy /etc/audit/audit.rules

-w /etc/selinux/ -p wa -k MAC-policy ①
```

① Ожидаемый вывод

Исправление

Вставьте следующую строку в файл **/etc/audit/audit.rules**:

```
-w /etc/selinux/ -p wa -k MAC-policy
```

1.2.18. Обеспечить сбор событий, связанных с удалением файлов пользователями

Описание

Отслеживайте все случаи использования системных вызовов, связанных с удалением или переименованием файлов и их свойств. Данная функция конфигурации позволяет отслеживать системные вызовы `unlink` (удалить файл), `unlinkat` (удалить свойство файла), `rename` (переименовать файл) и `renameat` (переименовать свойство файла) и наделяет их идентификатором delete.

Исправление

Выполните действия, указанные в разделе 4.1.14 документа CIS Distribution Independent Linux Benchmark v1.1.0.

1.2.19. Обеспечить сбор событий, связанных с удачными подключениями файловых систем

Описание

Отслеживайте использование системного вызова `mount`. Системный вызов `mount` (и `umount`) управляет подключением и отключением файловых систем. Рассматриваемые настройки позволяют настроить систему на создание записей аудита при использовании системного вызова `mount` непривилегированным пользователем.

Непривилегированные пользователи крайне редко подключают файловые системы. Хотя регистрация команд `mount` и позволяет системному администратору получить свидетельство того, что было произведено подключение внешних носителей (после подтверждения, что источником подключения является внешний носитель), данный факт не указывает на то, что на носитель были экспортированы данные. Чтобы это установить, системным администраторам понадобятся данные об успешных системных вызовах `open`, `creat` и `truncate`, которые требуют доступа на запись для файла с точки подключения файловой системы внешнего носителя. Это позволит с большой долей вероятности определить факт записи. Единственный достоверный способ — регистрировать все случаи успешной записи на внешний носитель. Данная практика может привести к быстрому заполнению журнала аудита, что не рекомендуется. Рекомендации по вариантам конфигурации с целью отслеживания экспорта данных на внешние носители в данное требование не входят.

Исправление

Выполните действия, указанные в разделе 4.1.13 документа CIS Distribution Independent Linux Benchmark v1.1.0.

1.2.20. Обеспечить фиксацию действий системных администраторов (sudolog)

Описание

Изменения в **/var/log/sudo.log** указывают на то, что либо администратор выполнил команду, либо целостность файла журнала была нарушена. Чтобы определить, были ли выполнены несанкционированные команды, администраторам нужно соотнести события, записанные в журналах аудита, с данными в **/var/log/sudo.log**.

Отслеживайте изменения в файле журнала **sudo**. Если система была правильно настроена на отключение команды `su`, любой администратор будет вынужден сначала войти в систему и только потом использовать `sudo` для выполнения привилегированных команд. Тогда все команды администраторов будут журналироваться в **/var/log/sudo.log**. Всякий раз, когда выполняется команда, будет создаваться событие аудита, а в открывшийся файл **/var/log/sudo.log** будет записана выполненная команда администрирования.

Проверка

Выполните указанную ниже команду и убедитесь, что в выводе содержится соответствующая запись:

```
grep actions /etc/audit/audit.rules

-w /var/log/sudo.log -p wa -k actions ①
```

① Ожидаемый вывод

Исправление

Вставьте следующую строку в файл /etc/audit/audit.rules:

```
-w /var/log/sudo.log -p wa -k actions
```

1.3. Конфигурация сети

1.3.1. Обеспечить журналирование подозрительных пакетов

Описание

Данная функция позволяет журналировать пакеты с немаршрутизируемыми адресами источников в журнал ядра.

Включение данной функции и журналирование таких пакетов позволит администратору распознать подмененные пакеты, посылаемые системе злоумышленником.

Проверка

Выполните указанные команды и убедитесь, что в выводе содержатся соответствующие записи:

```
sysctl net.ipv4.conf.all.log_martians
net.ipv4.conf.all.log_martians = 1 ①

sysctl net.ipv4.conf.default.log_martians
net.ipv4.conf.default.log_martians = 1 ①
```

① Ожидаемый вывод

Исправление

Настройте следующие параметры в файле **/etc/sysctl.conf**:

```
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.default.log_martians = 1
```

Запустите следующие команды, чтобы настроить активные параметры ядра:

```
/sbin/sysctl -w net.ipv4.conf.all.log_martians=1
/sbin/sysctl -w net.ipv4.conf.default.log_martians=1
/sbin/sysctl -w net.ipv4.route.flush=1
```

1.3.2. Обеспечить отклонение безопасных сообщений ICMP Redirect

Описание

Даже известные шлюзы могут быть скомпрометированы. Установка значения `0` для `net.ipv4.conf.all.secure_redirects` позволит защитить систему от обновлений таблиц маршрутизации потенциально скомпрометированными известными шлюзами.

Безопасное сообщение ICMP Redirect аналогично простому сообщению ICMP Redirect с единственным отличием: источником в первом случае являются шлюзы, входящие в список стандартных шлюзов. Предполагается, что эти шлюзы известны системе и скорее всего безопасны.

Проверка

Выполните указанные команды и убедитесь, что в выводе содержатся соответствующие записи:

```
sysctl net.ipv4.conf.all.secure_redirects
net.ipv4.conf.all.secure_redirects = 0 ①

sysctl net.ipv4.conf.default.secure_redirects
net.ipv4.conf.default.secure_redirects = 0 ①
```

① Ожидаемый вывод

Исправление

Настройте следующие параметры в файле **/etc/sysctl.conf**:

```
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.secure_redirects = 0
```

Запустите следующие команды, чтобы настроить активные параметры ядра:

```
/sbin/sysctl -w net.ipv4.conf.all.secure_redirects=0
/sbin/sysctl -w net.ipv4.conf.default.secure_redirects=0
/sbin/sysctl -w net.ipv4.route.flush=1
```

1.3.3. Обеспечить отклонение пакетов с маршрутизацией от источника

Описание

В сетевых подключениях маршрутизация от источника позволяет отправителю полностью или частично определять маршрут, по которому проходят пакеты по сети, в то время как пакеты с обычной маршрутизацией проделывают путь, заданный маршрутизаторами сети. В некоторых случаях у систем отсутствует возможность маршрутизации или они недоступны из ряда мест (в пример можно привести адреса частных сетей в сравнении с маршрутизируемыми через интернет), и потому возникает необходимость в пакетах с маршрутизацией от источника.

Установка значения `0` для `net.ipv4.conf.all.accept_source_route` и `net.ipv4.conf.default.accept_source_route` не позволит системе принимать пакеты с маршрутизацией от источника. Предположим, что система может направлять пакеты на адреса с маршрутизацией через интернет на одном интерфейсе и на адреса частных сетей на другом. Причем отсутствует возможность направлять пакеты от частных адресов к адресам с интернет-маршрутизацией и наоборот. В обычных условиях злоумышленник с адресов с интернет-маршрутизацией не мог бы использовать систему, чтобы добраться до систем с частными адресами. Однако, если пакеты с маршрутизацией от источника были бы разрешены, злоумышленник мог бы получить доступ к системам частных адресов, поскольку существовала бы возможность установки маршрута, позволяющая обойти протоколы маршрутизации, не допускающие такую возможность.

Проверка

Выполните указанные команды и убедитесь, что в выводе содержатся соответствующие записи:

```
sysctl net.ipv4.conf.all.accept_source_route
net.ipv4.conf.all.accept_source_route = 0 ①
```

```
sysctl net.ipv4.conf.default.accept_source_route
net.ipv4.conf.default.accept_source_route = 0 ①
```

① Ожидаемый вывод

Исправление

Настройте следующие параметры в файле **/etc/sysctl.conf**:

BASH

```
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0
```

Запустите следующие команды, чтобы настроить активные параметры ядра:

BASH

```
/sbin/sysctl -w net.ipv4.conf.all.accept_source_route=0
/sbin/sysctl -w net.ipv4.conf.default.accept_source_route=0
/sbin/sysctl -w net.ipv4.route.flush=1
```

1.3.4. Обеспечить отклонение сообщений ICMP Redirect

Описание

Злоумышленники могут воспользоваться поддельными сообщениями ICMP Redirect и внести изменения в таблицы маршрутизации системы, чтобы заставить их отсылать пакеты на некорректные сети, где они будут перехвачены.

Сообщения ICMP Redirect являются пакетами, передающими информацию о маршрутизации и сообщающие узлу, выполняющему роль маршрутизатора, о необходимости отправить пакет по альтернативному пути. Это дает возможность обновить таблицы маршрутизации системы при помощи стороннего маршрутизатора. При установке значения `0` для `net.ipv4.conf.all.accept_redirects` система перестанет принимать все сообщения ICMP Redirect и таким образом не позволит третьим лицам обновить таблицы маршрутизации системы.

Проверка

Выполните указанные команды и убедитесь, что в выводе содержатся соответствующие записи:

BASH

```
sysctl net.ipv4.conf.all.accept_redirects
net.ipv4.conf.all.accept_redirects = 0 ①

sysctl net.ipv4.conf.default.accept_redirects
net.ipv4.conf.default.accept_redirects = 0 ①
```

① Ожидаемый вывод

Исправление

Настройте следующие параметры в файле **/etc/sysctl.conf**:

```
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
```

Запустите следующие команды, чтобы настроить активные параметры ядра:

```
/sbin/sysctl -w net.ipv4.conf.all.accept_redirects=0
/sbin/sysctl -w net.ipv4.conf.default.accept_redirects=0
/sbin/sysctl -w net.ipv4.route.flush=1
```

1.3.5. Обеспечить отключение отправки сообщений Redirect

Описание

Сообщения ICMP Redirect используются для перенаправления данных маршрутизации другим узлам. Если сам узел не выступает в качестве маршрутизатора, а только в качестве узла, в отправке сообщений Redirect нет необходимости.

Злоумышленник может воспользоваться скомпрометированным узлом для отправки недействительных сообщений ICMP Redirect на другие маршрутизаторы с целью нарушить механизм маршрутизации и направить пользователей в специально сформированную им систему вместо легитимной.

Проверка

Выполните указанные команды и убедитесь, что в выводе содержатся соответствующие записи:

```
sysctl net.ipv4.conf.all.send_redirects
net.ipv4.conf.all.send_redirects = 0 ①

sysctl net.ipv4.conf.default.send_redirects
net.ipv4.conf.default.send_redirects = 0 ①
```

① Ожидаемый вывод

Исправление

Настройте следующие параметры в файле **/etc/sysctl.conf**:

```
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
```

Запустите следующие команды, чтобы настроить активные параметры ядра:

```
/sbin/sysctl -w net.ipv4.conf.all.send_redirects=0
/sbin/sysctl -w net.ipv4.conf.default.send_redirects=0
/sbin/sysctl -w net.ipv4.route.flush=1
```

1.3.6. Обеспечить фильтрацию пакетов по обратному пути

Описание

При установке значения `1` для `net.ipv4.conf.all.rp_filter` и `net.ipv4.conf.default.rp_filter` ядро Linux будет применять фильтрацию по обратному пути для проверки корректности получаемого пакета. В случае если обратный пакет не отправляется от того же интерфейса, что и соответствующий ему пакет источника, он отбрасывается (и журналируется при включенном параметре log_martians).

Установка значения `1` для `net.ipv4.conf.all.rp_filter` и `net.ipv4.conf.default.rp_filter` позволит помешать злоумышленникам направлять в систему специально сформированные пакеты, на которые невозможно откликнуться. Фильтрация пакетов по обратному пути не работает в случае, если применяется асимметричная маршрутизация, возникающая в результате использования динамических протоколов маршрутизации (bgp, ospf, etc) в системе. Применение фильтрации пакетов по обратному пути не возможно без нарушения работы асимметричной маршрутизации (если она используется в системе).

Проверка

Выполните указанные команды и убедитесь, что в выводе содержатся соответствующие записи:

```
sysctl net.ipv4.conf.all.rp_filter
net.ipv4.conf.all.rp_filter = 1 ①

sysctl net.ipv4.conf.default.rp_filter
net.ipv4.conf.default.rp_filter = 1 ①
```

① Ожидаемый вывод

Исправление

Настройте следующие параметры в файле **/etc/sysctl.conf**:

```
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
```

Запустите следующие команды, чтобы настроить активные параметры ядра:

```
/sbin/sysctl -w net.ipv4.conf.all.rp_filter=1
/sbin/sysctl -w net.ipv4.conf.default.rp_filter=1
/sbin/sysctl -w net.ipv4.route.flush=1
```

BASH

1.4. Обслуживание системы

1.4.1. Обеспечить для домашних каталогов пользователей назначение разрешений 750 или более строгих

Описание

Несмотря на то, что системный администратор может установить безопасные права доступа для домашних каталогов пользователей, сами пользователи могут без труда их переопределить.

Домашние каталоги пользователей, открытые на запись для всех или для какой-либо группы, могут позволить злоумышленнику украсть или изменить данные других пользователей, чтобы повысить свои привилегии.

Проверка

Полный сценарий аудита приведен в разделе 6.2.8 документа CIS Distribution Independent Linux Benchmark v1.1.0.

Исправление

Внесение глобальных изменений в домашние каталоги пользователей незаметно для самих пользователей может привести к непредсказуемым последствиям. Поэтому следует определить политику мониторинга, чтобы сообщать о правах доступа на файл пользователя и устанавливать порядок действий в соответствии с политикой организации.

1.4.2. Обеспечить наличие домашних каталогов у всех пользователей

Описание

Пользователи могут быть определены в **/etc/passwd** без домашнего каталога или с несуществующим каталогом.

Если домашний каталог пользователя не существует или же не назначен, пользователь будет помещен в каталог "/" и не сможет осуществлять запись в файлы либо иметь настроенные параметры локального окружения.

Проверка

Выполните следующий сценарий и убедитесь, что он не выдает результата:

```bash
#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid
dir; do
if [ $uid -ge 500 -a ! -d "$dir" -a $user != "nfsnobody" ]; then
echo "The home directory ($dir) of user $user does not exist."
fi
done
```

Исправление

Если пользователю назначен несуществующий домашний каталог, создайте его и убедитесь, что его владельцем является данный пользователь. Пользователи без назначенного домашнего каталога должны быть удалены или привязаны к соответствующему домашнему каталогу.

1.4.3. Обеспечить настройку безопасных разрешений на доступ к файлу /etc/group-

Описание

Файл **/etc/group-** содержит резервный список всех активных групп в системе.

Необходимо удостовериться, что файл **/etc/group-** защищен от неавторизованного доступа. Хотя по умолчанию он защищен, права на доступ к нему могут быть изменены случайно либо намеренно.

Проверка

Запустите следующую команду и убедитесь, что для UID и GID указано **0/root** и права на доступ определены как **600** или более строгие:

```bash
stat /etc/group-

Access: (0600/-rw-------) Uid: ( 0/ root) Gid: ( 0/ root) ①
```

① Ожидаемый вывод

Исправление

Чтобы установить права доступа для файла **/etc/group-**, выполните следующую команду:

```bash
chown root:root /etc/group-
chmod 600 /etc/group-
```

1.4.4. Обеспечить настройку безопасных разрешений на доступ к файлу /etc/passwd-

Описание

Файл **/etc/passwd-** содержит резервную копию данных об учетных записях.

Необходимо удостовериться, что файл **/etc/passwd-** защищен от неавторизованного доступа. Хотя по умолчанию он защищен, права на доступ к нему могут быть изменены случайно либо намеренно.

Проверка

Запустите следующую команду и убедитесь, что для UID и GID указано **0/root** и права на доступ определены как **600** или более строгие:

```
BASH
stat /etc/passwd-

Access: (0600/-rw-------) Uid: ( 0/ root) Gid: ( 0/ root) ①
```

① Ожидаемый вывод

Исправление

Чтобы установить права доступа для файла **/etc/passwd-**, выполните следующую команду:

```
BASH
chown root:root /etc/passwd-
chmod 600 /etc/passwd-
```

1.5. Первоначальная настройка

1.5.1. Обеспечить безопасную настройку /tmp

Описание

Каталог **/tmp** является общедоступным для записи и используется для временного хранения данных всеми пользователями и некоторыми приложениями.

Поскольку каталог **/tmp** открыт для записи всем пользователям, существует риск возникновения нехватки ресурсов. Для предотвращения подобной ситуации необходимо выделить под него отдельный раздел.

Нехватка места в каталоге **/tmp** представляет собой проблему независимо от того, какая файловая система используется в системе. Однако при стандартной установке дисковый каталог **/tmp** получит в распоряжение весь диск, поскольку на всем диске будет создан один единственный раздел "/". С другой стороны, **/tmp** в памяти, как, например, при использовании **tmpfs**, почти наверняка будет гораздо меньшего размера, что может значительно быстрее привести к заполнению файловой системы данными приложений. Размер каталога **/tmp** в **tmpfs** можно изменить с помощью параметра `size={size}` в строке **Options** файла **tmp.mount**.

Создание собственной файловой системы для **/tmp** позволит администратору установить опцию `noexec`, тем самым устранив вероятность того, что злоумышленник воспользуется каталогом для внедрения исполняемого кода. Дополнительно данная мера позволит предотвратить установку жесткой ссылки на системную программу `setuid`. После обновления жесткая ссылка оказалась бы взломанной, а злоумышленник получил бы экземпляр программы и возможность эксплуатировать имеющиеся в ней уязвимости. Если бы в программе оказалась известная уязвимость в области безопасности, злоумышленник мог бы воспользоваться ей.

Требование можно выполнить, установив **tmpfs** для **/tmp** либо выделив отдельный раздел для **/tmp**.

Проверка

Выполните следующую команду и убедитесь, что каталог **/tmp** подключен:

```
mount | grep /tmp

tmpfs on /tmp type tmpfs (rw,nosuid,nodev,noexec,relatime) ①
```

① Пример вывода

Исправление

Во время установки системы проведите настройку таблицы разделов, указав отдельный раздел для **tmp**.

Для исправления проблемы в уже установленных системах создайте новый раздел и установите необходимые параметры в файле **/etc/fstab**.

Подсистема systemd содержит службу tmp.mount, которую следует использовать вместо настройки /etc/fstab.

1.5.2. Обеспечить ограничение на формирование дампов памяти

Описание

Настройка жесткого (hard) ограничения для дампов памяти позволяет избежать переопределения пользователями переменной soft. При необходимости использования дампов памяти настройте ограничения для групп пользователей — см. limits.conf(5). Также применение значения 0 к переменной **fs.suid_dumpable** позволит предотвратить получение дампа ядра программами с атрибутом **setuid**.

Дамп памяти является содержимым памяти исполняемой программы. Обычно он требуется для определения причины, по которой работа программы была прекращена. Также он может использоваться для сбора конфиденциальной информации из файла ядра. Система

позволяет установить мягкое (soft) ограничение на дампы памяти, однако пользователи могут переопределять его.

Проверка

Выполните указанные команды и убедитесь, что в выводе содержатся соответствующие записи:

```
grep "hard core" /etc/security/limits.conf /etc/security/limits.d/*
* hard core 0 ①

sysctl fs.suid_dumpable
fs.suid_dumpable = 0 ①
```

① Ожидаемый вывод

Исправление

1. Вставьте следующую строку в файл **/etc/security/limits.conf** или какой-либо из файлов в каталоге **/etc/security/limits.d/**:

   ```
   * hard core 0
   ```

2. Настройте следующий параметр в файле **/etc/sysctl.conf**:

   ```
   fs.suid_dumpable = 0
   ```

3. Запустите следующую команду, чтобы настроить активный параметр ядра:

   ```
   sysctl -w fs.suid-dumpable=1
   ```

1.5.3. Обеспечить отдельный раздел для /home

Описание

Каталог **/home** используется для хранения на диске данных локальных пользователей.

Если система предназначена для поддержки локальных пользователей, рекомендуется создать отдельный раздел для каталога **/home**, чтобы предотвратить возникновение нехватки ресурсов и задать ограничения для типов файлов, которые разрешено хранить в **/home**.

Проверка

Выполните следующую команду и убедитесь, что каталог **/home** подключен:

```
mount | grep /home
```

```
/dev/xvdf1 on /home type ext4 (rw,nodev,relatime,data=ordered) ①
```

① Пример вывода

Исправление

Во время установки системы проведите настройку таблицы разделов, указав отдельный раздел для **/home**.

Для исправления проблемы в уже установленных системах создайте новый раздел и задайте необходимые настройки в файле **/etc/fstab**.

Подсистема systemd содержит службу **home.mount**, которую следует использовать вместо настройки /etc/fstab.

1.5.4. Обеспечить отдельный раздел для /var

Описание

Поскольку каталог **/var** может содержать файлы и каталоги, общедоступные для записи, существует риск возникновения нехватки ресурсов, если не выделить для него отдельный раздел.

Каталог **/var** используется программами-демонами и другими системными службами для временного хранения динамических данных. Некоторые каталоги, созданные данными процессами, могут быть доступны для записи всем пользователям.

Проверка

Выполните следующую команду и убедитесь, что каталог **/var** подключен:

BASH

```
mount | rep /var

/dev/xvdg1 on /var type ext4 (rw,relatime,data=ordered) ①
```

① Пример вывода

Исправление

Во время установки системы проведите настройку таблицы разделов, указав отдельный раздел для **/var**.

Для исправления проблемы в уже установленных системах создайте новый раздел и задайте необходимые настройки в файле **/etc/fstab**.

Подсистема systemd содержит службу **var.mount**, которую следует использовать вместо настройки /etc/fstab.

1.5.5. Обеспечить отдельный раздел для /var/log

Описание

Каталог **/var/log** используется системными службами для хранения данных журналов.

Существуют две важные причины хранения системных журналов в отдельном разделе: защита от возникновения нехватки ресурсов (журналы могут иметь довольно большой размер) и защита данных аудита.

Проверка

Выполните следующую команду и убедитесь, что каталог **/var/log** подключен:

```
mount | grep /var/log

/dev/xvdh1 on /var/log type ext4 (rw,relatime,data=ordered) ①
```

① Пример вывода

Исправление

Во время установки системы проведите настройку таблицы разделов, указав отдельный раздел для **/var/log**.

Для исправления проблемы в уже установленных системах создайте новый раздел и задайте необходимые настройки в файле **/etc/fstab**.

Подсистема systemd содержит службу **var-log.mount**, которую следует использовать вместо настройки /etc/fstab.

1.5.6. Обеспечить отдельный раздел для /var/log/audit

Описание

Демон аудита **auditd** хранит данные журналов в каталоге **/var/log/audit**.

Существуют две важные причины хранения данных, собранных **auditd**, в отдельном разделе: защита от возможной нехватки ресурсов (файл **audit.log** может иметь достаточно большой размер) и защита данных аудита. Демон аудита рассчитывает количество свободного дискового пространства и в соответствии с полученными результатами выполняет необходимые действия. Если другие процессы (такие как **syslog**) занимают место в том же разделе, что и auditd, его функционирование может быть нарушено.

Проверка

Выполните следующую команду и убедитесь, что каталог **/var/log/audit** подключен:

```
mount | grep /var/log/audit

/dev/xvdi1 on /var/log/audit type ext4 (rw,relatime,data=ordered) ①
```

① Пример вывода

Исправление

Во время установки системы проведите настройку таблицы разделов, указав отдельный раздел для **/var/log/audit**.

Для исправления проблемы в уже установленных системах создайте новый раздел и задайте необходимые настройки в файле **/etc/fstab**.

Подсистема systemd содержит службу **var-log-audit.mount**, которую следует использовать вместо настройки /etc/fstab.

1.5.7. Обеспечить установку пароля для начального загрузчика

Описание

Если пароль начального загрузчика системы настроен, то человеку, выполняющему перезагрузку, необходимо ввести пароль, чтобы получить возможность настраивать параметры загрузки через интерфейс командной строки.

Требование ввести пароль при исполнении программы начальной загрузки не позволит неавторизованным пользователям выполнять ввод параметров загрузки или менять загрузочный раздел диска. Таким образом, пользователи не смогут ослабить безопасность (например, отключить SELinux при загрузке).

Проверка

Выполните следующие команды и убедитесь, что вывод содержит соответствующие записи:

```
grep '^\s*password_pbkdf2' /boot/grub2/grub.cfg
password_pbkdf2 root ${GRUB2_PASSWORD} ①

grep "^\s*set superusers" /boot/grub2/grub.cfg
set superusers="root" ①
```

① Пример вывода

Исправление

1. Задайте пароль для grub следующей командой:

```
grub2-setpassword
```

2. Выполните перезагрузку.

```
reboot
```

BASH

1.6. Службы

1.6.1. Обеспечить отключение NFS

Описание

За исключением случаев, когда системе необходимо экспортировать общие ресурсы NFS или играть роль NFS-сервера, следует отключить это ПО, чтобы уменьшить потенциальную поверхность атаки.

Проверка

Проверьте состояние служб nfs:

```
systemctl is-enabled nfs-server.service
disabled ①

systemctl is-enabled nfs-blkmap.service
disabled ①
```

BASH

① Ожидаемый вывод

Исправление

Отключите необходимые службы. Например:

```
systemctl disable --now nfs-server
```

BASH

1.6.2. Обеспечить отключение сервера HTTP

Описание

HTTP- или веб-серверы предоставляют возможность размещать содержимое сайтов.

За исключением случаев, когда система играет роль веб-сервера, следует отключить службу **httpd** и удалить пакет HTTP, чтобы уменьшить потенциальную поверхность атаки.

Проверка

Проверьте состояние службы **httpd**:

```
systemctl is-enabled httpd
disabled ①
```

BASH

① Ожидаемый вывод

Исправление

Отключите службу **httpd**:

```
systemctl disable --now httpd
```
BASH

1.6.3. Обеспечить отсутствие установленного клиента telnet в системе

Описание

Пакет **telnet** содержит клиент Telnet, позволяющий пользователям осуществлять соединение с другими системами по протоколу Telnet.

Протокол Telnet является небезопасным и не использует шифрование. Использование среды передачи, в которой отсутствует шифрование данных, может позволить неавторизованному пользователю украсть учетные данные. Пакет SSH предоставляет шифрование сеанса и более высокий уровень безопасности.

Проверка

Убедитесь, что клиент telnet не установлен:

```
rpm -q telnet
```
BASH

Исправление

Удалите клиент telnet:

```
dnf remove -y telnet
```
BASH

2. Применение профилей безопасности

Профили безопасности позволяют автоматически применить набор рекомендаций из списка выше.

Применение профилей выполняется путем установки и запуска на хостах утилиты **zvirt-system-security-set**.

2.1. Профиль 1

2.1.1. Включенные настройки безопасности

▸ Доступ, аутентификация и авторизация

▸ Журналирование и аудит

▸ Конфигурация сети

▸ Обслуживание системы

▸ Первоначальная настройка

▸ Службы

2.1.2. Применение профиля

Порядок действий:

1. Подключитесь по SSH к хосту, на котором будет устанавливаться профиль.

   Для обеспечения должного уровня безопасности, профиль должен быть применен на всех хостах.

2. Скачайте из репозитория пакет с профилем безопасности:

   ```
   BASH
   wget https://repo-zvirt.orionsoft.ru/tools/system-security-set-1.0.5.gp-1136290.zvirt.el8.noarch.rpm
   ```

3. Установите пакет:

   ```
   BASH
   dnf install ./system-security-set-1.0.5.gp-1136290.zvirt.el8.noarch.rpm
   ```

   Пакет можно устанавливать в любой момент после развертывания хоста.

4. Запустите утилиту для применения профиля безопасности:

   ```
   BASH
   zvirt-system-security-set
   ```

   Данную утилиту можно запускать повторно, если требуется привести профиль ИБ к исходному состоянию.

2.2. Профиль 2

2.2.1. Включенные настройки безопасности

▸ Локальная аутентификация

▸ Службы

▸ Журналирование и аудит

▸ Встроенные средства защиты информации

2.2.2. Применение профиля

Порядок действий:

1. Подключитесь по SSH к хосту, на котором будет устанавливаться профиль.

   Для обеспечения должного уровня безопасности, профиль должен быть применен на всех хостах.

2. Скачайте из репозитория пакет с профилем безопасности:

   ```
   BASH
   wget https://repo-zvirt.orionsoft.ru/tools/system-security-set-1.0.6.ps-1136291.zvirt.el8.noarch.rpm
   ```

3. Установите пакет:

   ```
   BASH
   dnf install ./system-security-set-1.0.6.ps-1136291.zvirt.el8.noarch.rpm
   ```

   Пакет можно устанавливать в любой момент после развертывания хоста.

4. Запустите утилиту для применения профиля безопасности:

   ```
   BASH
   zvirt-system-security-set
   ```

   Данную утилиту можно запускать повторно, если требуется привести профиль ИБ к исходному состоянию.

TPM и шифрование дисков

Формат **Linux Unified Key Setup-on-disk (LUKS)** позволяет шифровать блочные устройства и предоставляет набор инструментов, упрощающих управление зашифрованными устройствами.

PBD (Policy-Based Decryption) это набор технологий, которые позволяют разблокировать зашифрованные корневые и дополнительные тома жестких дисков на физических и виртуальных машинах. PBD использует различные методы разблокировки, например, устройство **Trusted Platform Module (TPM)**.

В zVirt реализация PBD состоит из **платформы Clevis** и **подключаемых модулей pin**. Каждый pin обеспечивает отдельную возможность разблокировки, например, **tpm2** позволяет разблокировать с использованием политик **TPM2**.

TPM или Trusted Platform Module– это набор спецификаций от **Trust Computing Group (TCG)**, разработанный независимо от операционной системы. Такие спецификации используются для разработки криптопроцессора (аппаратного или программного), функция которого заключается в защите платформы (аппаратной или программной, иначе виртуальной машины) с помощью криптографических ключей и операций. TPM не используется для шифрования/дешифрования наших данных на жестком диске; это аппаратное обеспечение, содержащее секретные ключи, которые используются программным компонентом для фактического шифрования и дешифрования на лету.

TPM поддерживают не все ОС.

1. Шифрование дисков хоста

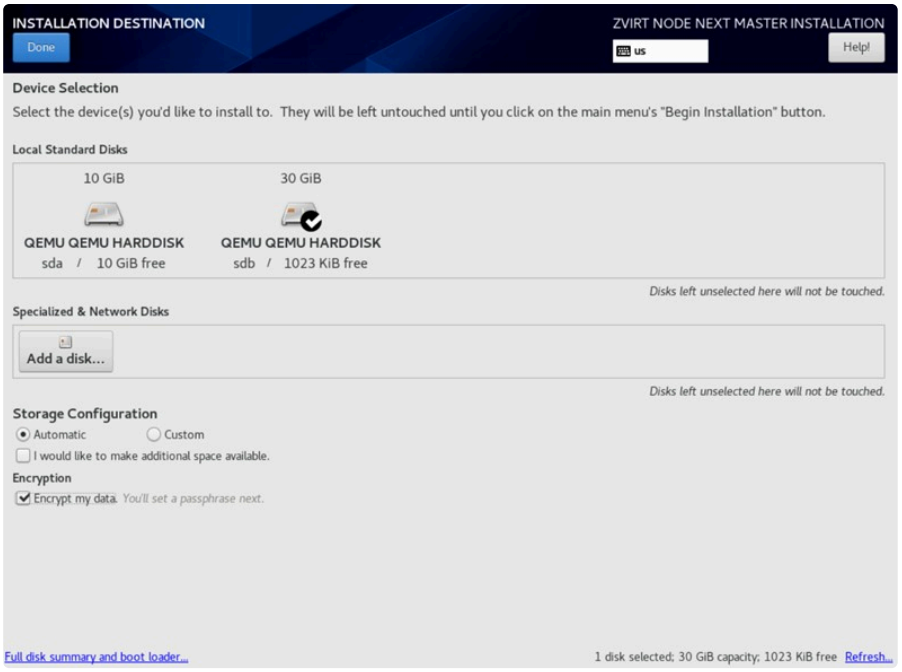
Требования:

1. Доступное устройство, совместимое с **TPM 2.0**.
2. Система с 64-разрядной архитектурой **Intel** или 64-разрядной архитектурой **AMD**.

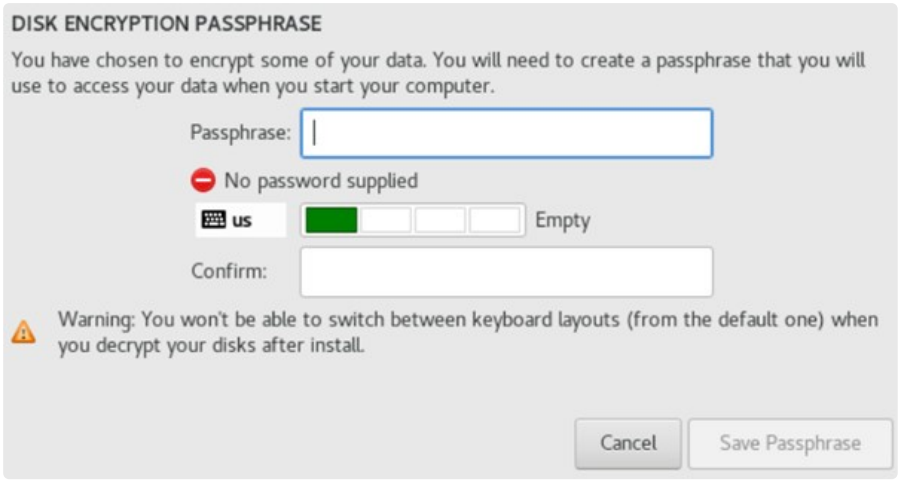
Методика:

1. Включить модуль TPM в BIOS/UEFI.

   Точные шаги для этой процедуры будут зависеть от вашего BIOS, вашей материнской платы, версии модуля **TPM**, поэтому обратитесь к руководству по материнской плате.
2. При установке ОС zVirt Node во время разбиения дисков выберите параметр “Encrypt my data”:



Введите фразу-пароль:



3. При загрузке системы после завершения установки введите фразу-пароль для входа в систему (Фраза-пароль будет запрашиваться при каждом запуске системы).

2. Настройка автоматической разблокировки дисков с помощью TPM

1. Убедимся может ли ядро правильно видеть модуль TPM:

```
dmesg | grep -i tpm
```

Если все работает корректно, то команда должна вывести выпуск модуля TPM:

```
Mar 17 20:37:15 vmm kernel: tpm_tis 00:05: 2.0 TPM (device-id 0xD, rev-id xy)
```

Другой способ - проверить, есть ли в **/dev/** устройство **tpm0**:

```
ls /dev/tpm0
```

2. Чтобы автоматически разблокировать существующий том, зашифрованный **LUKS**, установите подпакет **clevis-luks**:

```
yum install clevis-luks
```

3. Определите том, зашифрованный **LUKS**.

```
lsblk
```

В следующем примере блочное устройство упоминается как **/dev/sda3**:

```
[root@host1 ~]# lsblk
NAME                                                  MAJ:MIN RM   SIZE RO TYPE  MOUNTPOINT
sda                                                     8:0    0 222.6G  0 disk
├─sda1                                                  8:1    0   600M  0 part  /boot/efi
├─sda2                                                  8:2    0     1G  0 part  /boot
└─sda3                                                  8:3    0   221G  0 part
  └─luks-c63545dd-b4ef-4ee8-aea6-c4e92f7aa9e5         253:0    0   221G  0 crypt
    ├─znn_host1-pool00_tmeta                          253:1    0     1G  0 lvm
    │ └─znn_host1-pool00-tpool                        253:3    0 172.3G  0 lvm
    │   ├─znn_host1-zvirt--node--ng--3.0--0.20220527.0+1 253:4  0 135.3G  0 lvm   /
    │   ├─znn_host1-pool00                            253:6    0 172.3G  1 lvm
    │   ├─znn_host1-home                              253:7    0     1G  0 lvm   /home
    │   ├─znn_host1-tmp                               253:8    0     1G  0 lvm   /tmp
    │   ├─znn_host1-var                               253:9    0    15G  0 lvm   /var
    │   ├─znn_host1-var_crash                         253:10   0    10G  0 lvm   /var/crash
    │   ├─znn_host1-var_log                           253:11   0     8G  0 lvm   /var/log
    │   └─znn_host1-var_log_audit                     253:12   0     2G  0 lvm   /var/log/audit
    ├─znn_host1-pool00_tdata                          253:2    0 172.3G  0 lvm
    │ └─znn_host1-pool00-tpool                        253:3    0 172.3G  0 lvm
    │   ├─znn_host1-zvirt--node--ng--3.0--0.20220527.0+1 253:4  0 135.3G  0 lvm   /
    │   ├─znn_host1-pool00                            253:6    0 172.3G  1 lvm
    │   ├─znn_host1-home                              253:7    0     1G  0 lvm   /home
    │   ├─znn_host1-tmp                               253:8    0     1G  0 lvm   /tmp
    │   ├─znn_host1-var                               253:9    0    15G  0 lvm   /var
    │   ├─znn_host1-var_crash                         253:10   0    10G  0 lvm   /var/crash
    │   ├─znn_host1-var_log                           253:11   0     8G  0 lvm   /var/log
    │   └─znn_host1-var_log_audit                     253:12   0     2G  0 lvm   /var/log/audit
    └─znn_host1-swap                                  253:5    0     4G  0 lvm   [SWAP]
```

4. Привяжите том к устройству **TPM 2.0**:

```
clevis luks bind -d /dev/sda3 tpm2 '{"hash":"sha256","key":"rsa"}'
```

Эта команда выполняет четыре шага:

- Создает новый ключ с той же энтропией, что и главный ключ LUKS.
- Шифрует новый ключ с помощью Clevis.
- Сохраняет объект Clevis JWE в токене заголовка LUKS 2 или использует LUKSMeta, если используется заголовок LUKS 1, отличный от стандартного.
- Включает новый ключ для использования с LUKS.

В качестве альтернативы, если вы хотите привязать данные к определенным состояниям регистров конфигурации платформы (PCR), а значения **pcr_bank** и **pcr_ids** - к команде `clevis luks bind`:

```
clevis luks bind -d /dev/sda3 tpm2
```

```
‘{“hash”:”sha256”,”key”:”rsa”,”pcr_bank”:”sha256”,”pcr_ids”:”0,1”}’
```

Platform Configuration Register (PCR)

Киптографическая запись (изменения) состояния ПО. Регистры хранят ключи для проверки ПО при запуске системы. Если значения хэшей PCR не соответствуют политике, используемой при запечатывании, криптографические ключи, запечатанные с определённым набором значений PCR работать не будут.

5. Теперь том можно разблокировать с помощью вашего существующего пароля, а также с помощью политики Clevis.
6. Чтобы разрешить системе загрузки обрабатывать привязку диска, используйте инструмент dracut в уже установленной системе:

```
yum install clevis-dracut
dracut -fv --regenerate-all
```

dracut

Утилита создания initramfs (initial RAM disk image, загружаемый в оперативную память файл с образом файловой системы), используемого при загрузке Linux в качестве первоначальной корневой файловой системы. Загрузчик загружает в память ядро и initramfs, монтирует временную корневую файловую систему и передаёт управление ядру.
Задача **initramfs** - обеспечить хранение скриптов, программ, модулей ядра и прочих файлов, необходимых для загрузки драйверов, инициализации сетевых устройств, видео, устройств хранения, обработки сложных случаев.

3. Проверка работоспособности

Перезагружаем хост. При появлении запроса на ввод фразы-пароля, не вводим его самостоятельно. Через некоторый период времени (~ 1 минута) сработает TPM и система запустится самостоятельно.

4. Возможные проблемы

```
clevis luks bind -d /dev/sda3 tpm2 '{"hash":"sha256","key":"rsa"}'
```

4.1. Проблема

```
Warning: Value 512 is outside of the allowed entropy range, adjusting it.
WARNING:esys:src/tss2-esys/api/Esys_Create.c:375:Esys_Create_Finish() Received
```

```
TPM Error
ERROR:esys:src/tss2-esys/api/Esys_Create.c:375:Esys_Create()Esys Finish
ErrorCode (0x00000921)
ERROR: Esys_Create(0x921) - tpm:warn(2.0): authorizations for objects subjects
to DA protection are not allowed at thes time because the TPM is in DA lockout
mode
ERROR: Unable to run tpm2_create
Creating TPM2 object for jwk failed!
```

4.2. Решение

```
echo 5 > /sys/class/tpm/tpm0/ppi/request
reboot
```

После перезагрузки система предложит очистить информацию на TPM или отклонить этот запрос и продолжить. Выбираем первый вариант.

После этого TPM сбрасывается, и команда работает корректно.

5. Чтобы убедиться, что объект Clevis JWE успешно помещен в заголовок LUKS

```
clevis luks list -d /dev/sda3
```

Вывод:

```
tpm2 '{"hash":"sha256","key":"rsa"}'
```

6. Рекомендуемый способ удаления Clevis pin с тома, зашифрованного LUKS (отключение автоматической разблокировки)

Работает как для томов **LUKS1**, так и для томов **LUKS2**. Команда удаляет метаданные, созданные на этапе привязки, и стирает слот для ключей 1 на устройстве **/dev/sda3**:

```
clevis luks unbind -d /dev/sda3 -s 1
```

7. Удаление вручную Clevis pin с тома, зашифрованного LUKS

7.1. Требования

Том, зашифрованный **LUKS**, с привязкой **Clevis**.

Методика:

1. Проверьте, какой версией **LUKS** зашифрован том, например **/dev/sda3**, и определите слот и токен, привязанный к **Clevis**:

   ```
   clevis luksDump /dev/sd3
   ```

   Вывод:

2. В случае шифрования LUKS2 удалите токен:

   ```
   cryptsetup token remove --token-id 0 /dev/sda3
   ```

3. Если ваше устройство зашифровано с помощью **LUKS1**, на что указывает строка **Version: 1** в выходных данных команды **cryptsetup luksDump**, выполните этот дополнительный шаг:

   ```
   luksmeta wipe -d /dev/sda3 -s 1
   ```

4. Сотрите слот для ключей, содержащий кодовую фразу **Clevis**:

   ```
   cryptsetup luksKillSlot /dev/sda3 1
   ```

   После этих процедур автоматическая разблокировка дисков с помощью TPM работать не будет.

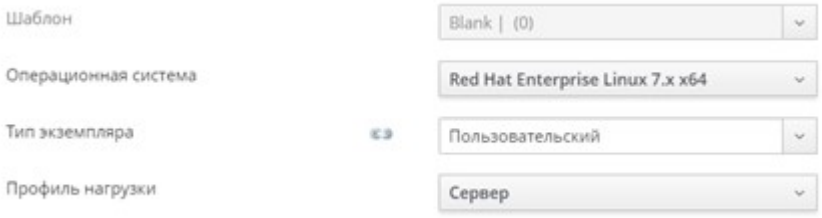
8. Шифрование дисков виртуальной машины и настройка автоматической расшифровки с помощью TPM

8.1. Требования

При создании ВМ:

1. Эмуляция TPM работает только с прошивкой **UEFI** (**Система > Тип BIOS**):

2. Необходимо указать Операционную систему ВМ (**Общее > Операционная система**):



3. Включить TPM в настройках виртуальной машины (**Выделение ресурсов > Модуль TPM**):

9. Настройка шифрования дисков ВМ

9.1. Шифрование дисков с данными используя LUKS2

9.1.1. Требования

1. Блочное устройство содержит файловую систему.
2. Вы создали резервную копию своих данных.

9.1.2. Методика

1. Размонтируйте все файловые системы, которые необходимо зашифровать:

```
umount /dev/sdc1
```

2. Освободите место для хранения заголовка LUKS. Выберите один из следующих вариантов, который соответствует вашему сценарию:
   - В случае шифрования логического тома вы можете расширить логический том без изменения размера файловой системы:

```
lvextend -L +32M vg00/lv00
```

- Расширьте раздел с помощью инструментов управления разделами, таких как **fstab**.
- Уменьшите размер файловой системы на устройстве. Вы можете использовать утилиту **resize2fs** для файловых систем **ext2**, **ext3** или **ext4**. Обратите внимание, что вы не можете уменьшить размер файловой системы XFS.

3. Инициализируйте шифрование:

```
cryptsetup reencrypt --encrypt --init-only --reduce-device-size 32M
/dev/sdc1 sdc1_encrypted
```

Команда запросит у вас кодовую фразу и запустит процесс шифрования.

4. Примонтируйте устройство:

```
mount /dev/mapper/sdc1_encrypted /mnt/sdc1_encrypted
```

5. Запустите онлайн-шифрование:

```
cryptsetup reencrypt --resume-only /dev/sdc1
```

9.2. Шифрование пустых дисков используя LUKS2

9.2.1. Требование

1. Пустое блочное устройство

Методика:

1. Настройте раздел как зашифрованный раздел **LUKS**:

```
cryptsetup luksFormat /dev/sdc1
```

2. Откройте зашифрованный раздел **LUKS**:

```
cryptsetup open /dev/sdc1 sdc1_encrypted
```

Эта команда разблокирует раздел и сопоставит его с новым устройством с помощью средства сопоставления устройств. Это предупреждает ядро о том, что устройство является зашифрованным устройством и должно быть адресовано через LUKS с использованием **/dev/mapper/device_mapped_name**, чтобы не перезаписывать зашифрованные данные.

3. Чтобы записать зашифрованные данные в раздел, к нему необходимо получить доступ через сопоставленное имя устройства. Для этого вы должны создать файловую систему.

```
mkfs –t ext4 /dev/mapper/sdc1_encrypted
```

4. Примонтируем устройство:

```
mount /dev/mapper/sdc1_encrypted mount-point
```

Настройка автоматической разблокировки дисков с помощью TPM аналогична настройке для хоста

10. Выводы

1. Шифрование дисков хоста в zVirt работает.
2. Автоматическая разблокировка дисков хоста с помощью TPM настраивается и работает.
3. Для хоста возможна только аппаратная реализация TPM.
4. Автоматическая разблокировка дисков ВМ с помощью TPM настраивается и работает.