масштаб
научно-
исследовательский
институт

VeiL®

Enterprise Cloud Platform

Руководство системного программиста

ИСКП.00021-01 32 01

Листов 65

2020

АННОТАЦИЯ

Данный документ является руководством системного программиста для Enterprise Cloud Platform Veil (облачной платформы корпоративного уровня Veil), далее по тексту – ECP Veil или программа. ECP Veil предназначена для создания и администрирования виртуальной инфраструктуры на базе универсальных серверных платформ с архитектурой x86-64.

Документ описывает назначение, структуру ECP Veil, последовательность установки и настройки программы, рекомендации и требования, исполнение которых необходимо для корректного функционирования ECP Veil.

Настоящее руководство входит в состав эксплуатационной документации и рассчитано на системного программиста, имеющего навыки работы на персональной электронно-вычислительной машине (ПЭВМ) и администрирования операционных систем (ОС) семейства Linux.

СОДЕРЖАНИЕ

Лист

1. ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

1.1. Назначение программы

1.1.1. ECP Veil предназначена для решения следующих задач:

– повышение эффективности использования вычислительных ресурсов – возможность запуска нескольких виртуальных серверов (машин) на одном физическом сервере;

– обеспечение выполнения на одном физическом сервере несовместимых приложений – возможность запуска операционных систем семейства Linux и Windows, а также рабочих станций, шлюзов, баз данных и других приложений, несовместимых в рамках одного экземпляра ОС;

– организация общего виртуального пространства – возможность объединять физические серверы в кластер единого управления (далее – кластер), который представляется как единый пул для работы на нем виртуальных машин (ВМ) с пользовательскими приложениями;

– повышение доступности и обеспечение непрерывности работы приложений – предоставление функций переноса ВМ на другой сервер кластера без прерывания выполнения пользовательского приложения и самовосстановления ВМ на резервных серверах в кластере;

– повышение удобства управления вычислительными ресурсами – управление несколькими физическими серверами с централизованного Web-интерфейса с повышенной степенью автоматизации для сокращения времени администрирования и понижения порога вхождения персонала.

1.1.2. ECP Veil обеспечивает создание и администрирование виртуальной инфраструктуры на одном физическом сервере или на группе физических серверов.

1.1.3. ECP Veil обеспечивает создание и управление следующими типами объектов вычислительной инфраструктуры:

– физический сервер или вычислительный узел (физический сервер, входящий в состав логической группы);

– виртуальная машина;

– виртуальная сеть;

– пул хранения данных;

– виртуальный диск;

– образ оптического диска.

1.1.4. ECP Veil обеспечивает следующие возможности работы с ВМ:

– запуск 32- и 64-битных гостевых ОС на ВМ;

– инсталляции ОС внутри ВМ с образа оптического диска в формате ISO 9660 и UDF.

1.1.5. ECP Veil обеспечивает следующие виды организации хранилищ данных:

– необщие хранилища;

– общие хранилища.

1.1.6. ECP Veil обеспечивает использование локальных групп логических томов (LVM – Logical Volume Manager) на вычислительных узлах в качестве локальных (необщих) хранилищ данных.

1.1.7. ECP Veil обеспечивает поддержку следующих типов переноса ВМ между физическими серверами:

– перенос без приостановки работы ВМ («live migration» – «живая миграция»);

– перенос с приостановкой работы ВМ.

1.1.8. ECP Veil при помощи средств интерфейса управления обеспечивает выполнение следующих операций:

– создание ВМ с инсталляцией с образа оптического диска;

– уничтожение ВМ (с сохранением ее виртуального жестокого диска и без него);

– редактирование параметров ВМ;

– запуск ВМ;

– остановка ВМ;

– перезагрузка ВМ;

– миграция ВМ на другой сервер;

– создание копии состояния ВМ (снэпшот ВМ);

– восстановление состояния текущей ВМ из копии.

1.1.9. ECP Veil при создании ВМ обеспечивает возможность задания следующих параметров:

– имя ВМ;

– описание ВМ;

– количество виртуальных процессоров (vCPU);

– количество оперативной памяти;

– количество дискового пространства;

– количество сетевых интерфейсов и их сопоставление с виртуальными сетями;

– вычислительный узел для запуска ВМ (из состава кластера);

– выбор существующего или создание нового виртуального диска;

– пул для хранения виртуального диска.

1.1.10. ECP Veil обеспечивает возможность с помощью опции при создании ВМ задавать количество виртуальных процессоров.

1.1.11. ECP Veil при помощи средств интерфейса управления обеспечивает выполнение следующих операций над виртуальными дисками:

– создание;

– уничтожение;

– подключение диска к ВМ;

– отключение диска от ВМ.

1.1.12. ECP Veil при создании виртуального диска обеспечивает возможность задать следующие параметры:

– имя виртуального диска;

– пул хранения для размещения виртуального диска;

– количество дисковой памяти.

1.1.13. ECP Veil обеспечивает возможность работы ВМ в режиме высокой доступности. Работа ВМ в режиме высокой доступности осуществляется путём автоматического перезапуска на резервном вычислительном узле виртуальных машин, которые были запущены на отказавшем вычислительном узле.

Примечания:

1. Работа ВМ в режиме высокой доступности возможна только при хранении виртуальных дисков данной ВМ на общем хранилище.

2. Высокая доступность обеспечивается только при объединении физических серверов в кластерную систему.

1.1.14. ECP Veil обеспечивает время запуска процедуры восстановления работы ВМ, запущенной в режиме высокой доступности, не более 5 мин.

1.1.15. ECP Veil обеспечивает возможность шифрования канала управления средствами протокола HTTPS.

1.1.16. ECP Veil обеспечивает вывод в интерфейс управления информации о текущем состоянии каждого физического сервера в кластере. Информация о каждом физическом сервере содержит:

– имя физического сервера;

– описание физического сервера;

– текущее состояние (доступен, недоступен);

– время с момента последнего включения;

– количество ВМ;

– график загрузки процессора (в процентах);

– график загрузки оперативной памяти (в процентах).

1.1.17. ECP Veil обеспечивает вывод в интерфейс управления следующей информации о каждой ВМ:

– имя ВМ;

– описание ВМ;

– текущее состояние (включена, выключена, приостановлена);

– время с момента последнего включения;

– дата создания ВМ.

1.1.18. ECP Veil обеспечивает доступ к локальным консолям ВМ через Web-интерфейс управления средствами протокола SPICE.

1.1.19. ECP Veil обеспечивает занесение в журнал записей о следующих событиях:

– авторизация пользователя в интерфейсе управления;

– ошибка аутентификации пользователя;

– изменение состояния физического сервера (доступен, недоступен);

– добавление нового физического сервера;

– удаление физического сервера;

– время создания ВМ;

– запуск ВМ;

– остановка ВМ;

– уничтожение ВМ;

– миграция ВМ;

– создание копии состояния ВМ (снэпшот ВМ).

1.1.20. ECP Veil обеспечивает использование внешних систем хранения данных, подключаемых по протоколу NFS, в качестве общих хранилищ.

1.1.21. ECP Veil обеспечивает синхронизацию размера окна Web-браузера с окном локальной консоли гостевой ОС при доступе к ВМ через Web-интерфейс управления средствами протокола SPICE.

1.1.22. ECP Veil обеспечивает возможность подключения к локальным консолям ВМ через «тонкого клиента» средствами протокола SPICE.

1.1.23. ECP Veil обеспечивает возможность подключения «тонких клиентов» к локальным консолям ВМ только с разрешенных IP-адресов.

1.1.24. ECP Veil обеспечивает возможность создания копии виртуального диска или образа оптического диска в том же или в другом пуле хранения данных.

Примечание. Операция переноса осуществляется только для виртуальных дисков и образов оптических дисков, не подключенных к ВМ.

1.1.25. В ECP Veil реализован распределенный коммутатор для обеспечения централизованного управления по созданию и администрированию виртуальных сетей, а также по подключению к ним ВМ.

1.1.26. Распределенный коммутатор в ECP Veil обеспечивает:

– механизм реализации единого виртуального сетевого пространства на серверах кластера в рамках создания виртуальных сетей;

– создание и настройку сетевых политик виртуальных локальных сетей (VLAN);

– создание агрегированных физических интерфейсов.

1.1.27. ECP Veil обеспечивает выбор загрузки ВМ в режиме Legacy-MBR или UEFI.

1.1.28. ECP Veil обеспечивает возможность с помощью опции задавать тип виртуального графического адаптера. В ECP Veil реализована поддержка следующих типов виртуальных графических адаптеров:

– cirrus;

– vga;

– qxl;

– virtio.

1.1.29. ECP Veil обеспечивает при создании ВМ выбор готовых настроек виртуального аппаратного обеспечения для ОС семейств Windows и Linux.

1.1.30. ECP Veil обеспечивает управление виртуальной инфраструктурой с централизованного графического Web-ориентированного интерфейса.

1.1.31. ECP Veil обеспечивает добавление физических серверов в виртуальную инфраструктуру из интерфейса управления в качестве вычислительных ресурсов и ресурсов хранения данных для размещения на них ВМ.

1.1.32. ECP Veil обеспечивает создание ВМ на физических серверах виртуальной инфраструктуры из интерфейса управления.

1.1.33. ECP Veil обеспечивает добавление физических серверов в виртуальную инфраструктуру.

Примечание. Перед добавлением физического сервера, на нем предварительно должно быть установлено программное обеспечение ECP Veil.

1.1.34. ECP Veil обеспечивает удаление физических серверов из виртуальной инфраструктуры через интерфейс управления.

1.1.35. ECP Veil обеспечивает создание в интерфейсе управления логических групп физических серверов и внешних систем хранения данных, находящихся на географически удаленных друг от друга площадках (далее – локации).

1.1.36. ECP Veil обеспечивает возможность добавления физических серверов и внешних систем хранения данных в локации и удаления из них.

1.1.37. ECP Veil обеспечивает создание в интерфейсе управления логических групп из физических серверов и внешних систем хранения данных, реализующих отдельные функции (далее – кластеры).

1.1.38. ECP Veil обеспечивает возможность использования следующих функций в рамках кластеров:

– миграция ВМ;

– высокая доступность ВМ;

– общий виртуальный распределенный коммутатор;

– учет административных правил размещения ВМ.

1.1.39. ECP Veil обеспечивает возможность задания идентификаторов (далее – тегов) физических серверов и ВМ.

1.1.40. ECP Veil обеспечивает создание кластеров с количеством физических серверов, начиная с двух.

1.1.41. ECP Veil обеспечивает возможность ограничения размещения ВМ на физическом сервере, если у них соответствуют или не соответствуют теги при включённой функции учета административных правил размещения ВМ в рамках кластера.

1.1.42. Интерфейс управления ECP Veil реализован на русском языке.

1.1.43. ECP Veil обеспечивает подключение внешних блочных разделов энергонезависимых запоминающих устройств (далее – LUN) в качестве виртуальных дисков ВМ по протоколу iSCSI.

1.1.44. ECP Veil обеспечивает использование внешних систем хранения данных, подключаемых по протоколу iSCSI, в качестве общих хранилищ для создания пулов хранения данных.

1.1.45. ECP Veil обеспечивает возможность подключения централизованной системы хранения данных (ЦСХД) с использованием встроенного API «Raidix» по протоколу iSCSI.

1.1.46. ECP Veil обеспечивает возможность автоматического определения реплицируемых и реплицированных LUN из списка обнаруженных на ЦСХД с использованием встроенного API «Raidix».

1.1.47. ECP Veil обеспечивает возможность создания катастрофоустойчивой ВМ на базе реплицируемого и реплицированного LUN ЦСХД, подключённых к разным локациям.

1.1.48. ECP Veil обеспечивает возможность миграции катастрофоустойчивой ВМ между локациями.

1.1.49. ECP Veil обеспечивает возможность восстановления катастрофоустойчивой ВМ между локациями.

1.1.50. ECP Veil обеспечивает возможность переключения реплицируемого LUN в режим реплицированного LUN и, наоборот, с использованием встроенного API «Raidix».

1.1.51. ECP Veil обеспечивает возможность пользователю восстановить программный модуль управления (далее – контроллер) на резервном физическом сервере из состава виртуальной инфраструктуры, в случае отказа основного физического сервера, на котором размещен контроллер.

1.1.52. В ECP Veil реализована возможность выбора резервного физического сервера из состава виртуальной инфраструктуры, на котором пользователь может восстановить контроллер.

1.1.53. ECP Veil обеспечивает возможность перемещения контроллера на другой физический сервер из состава виртуальной инфраструктуры без остановки работы ВМ.

1.1.54. ECP Veil обеспечивает сетевую доступность контроллера после его перемещения на другой физический сервер.

1.1.55. ECP Veil обеспечивает возможность мониторинга по протоколу SNMP компонентов виртуальной инфраструктуры из ее состава.

1.1.56. ECP Veil обеспечивает организацию оверлейной L2-сети между физическими серверами, расположенными в разных локациях.

1.1.57. ECP Veil обеспечивает организацию оверлейной L2-сети между ВМ, запущенными на физических серверах, расположенными в разных локациях.

1.1.58. ECP Veil обеспечивает проверку на совместимость и соответствие физических серверов и ВМ перед их переносом.

1.1.59. ECP Veil обеспечивает поддержку ролевой модели безопасности для управления доступом компонентов виртуальной инфраструктуры в интерфейсе управления.

1.1.60. ECP Veil обеспечивает возможность фильтрации пакетного сетевого трафика, поступающего из сети, внешней по отношению к виртуальной.

Примечание. Внешней сетью считают сеть, не принадлежащую единым сетевым пространствам, определенным виртуальными распределенными коммутаторами.

1.1.61. В ECP Veil критерии фильтрации основываются на соответствии или несоответствии пакетов поступающего сетевого трафика следующим параметрам:

– IP-адрес источника;

– IP-адрес назначения;

– порт источника;

– порт назначения;

– имя сетевого интерфейса источника;

– имя сетевого интерфейса назначения;

– протокол.

1.1.62. ECP Veil обеспечивает процедуры корректного и принудительного перезапуска физического сервера, а также процедуры корректного и принудительного выключения физического сервера в виртуальной инфраструктуре из интерфейса управления виртуальной инфраструктурой.

1.1.63. ECP Veil обеспечивает процедуры корректного и принудительного перезапуска физического сервера, а также процедуры корректного и принудительного выключения физического сервера через интерфейс IPMI.

1.1.64. ECP Veil при корректном выключении или перезапуске физического сервера из интерфейса управления обеспечивает корректное завершение работы всех ВМ, запущенных на выключаемом или перезапускаемом сервере.

1.1.65. ECP Veil обеспечивает принудительное выключение ВМ, в случае если ВМ не завершает свою работу в период времени, определенный таймаутом, при выполнении корректных процедур выключения или перезапуска физического сервера из интерфейса управления виртуальной инфраструктурой.

1.1.66. ECP Veil поддерживает и обеспечивает:

– выдачу ВМ IP-адресов, маски сети, IP-адреса шлюза «по умолчанию» и IP-адресов DNS-серверов средствами протокола DHCP или иными средствами;

– настройку диапазона IP-адресов, маски сети, IP-адреса шлюза «по умолчанию» и IP-адресов DNS-серверов, выдаваемых ВМ из графического интерфейса.

1.1.67. ECP Veil поддерживает и обеспечивает:

– возможность преобразования частных IP-адресов ВМ в публичные (технология NAPT);

– настройку преобразования частных IP-адресов ВМ в публичные (технология NAPT).

1.1.68. ECP Veil обеспечивает возможность:

– задания и изменения IP-адресов DNS-серверов для физических серверов виртуальной инфраструктуры;

– смены IP-адреса интерфейса управления на физических серверах из состава виртуальной инфраструктуры без остановки её работы и переконфигурации.

1.1.69. ECP Veil обеспечивает интеграцию со службой каталогов для хранения учетных записей и данных пользователей (LDAP или AD).

1.1.70. ECP Veil обеспечивает настройку статических маршрутов из интерфейса управления виртуальной инфраструктурой.

1.1.71. ECP Veil обеспечивает добавление виртуальной звуковой карты в ВМ.

1.1.72. ECP Veil обеспечивает монополизацию устройств, подключенных к разъемам PCI и PCI-E, виртуальными машинами.

1.1.73. ECP Veil обеспечивает:

– возможность загрузки виртуальных дисков в выбранный пул данных в форматах «vmdk» и «Qcow2» через графический Web-интерфейс;

– конвертацию виртуальных дисков формата «vmdk» в формат «Qcow2» при загрузке через графический Web-интерфейс;

– возможность загрузки образов оптических дисков в выбранный пул данных в форматах «ISO» и «UDF» через графический Web-интерфейс.

1.1.74. ECP Veil имеет возможность установки с USB-накопителя.

1.1.75. ECP Veil позволяет использовать до 480 физических процессоров, ядер или потоков в качестве виртуальных процессоров ВМ на одном физическом сервере.

1.1.76. ECP Veil позволяет использовать виртуальными машинами до 12 Тбайт физической оперативной памяти на одном физическом сервере.

1.1.77. ECP Veil позволяет запускать до 1000 ВМ на одном физическом сервере.

1.1.78. ECP Veil обеспечивает создание копий ВМ без прерывания работы оригинальной ВМ.

Примечание. Это выполняется только в том случае, если виртуальные диски хранятся в виде файлов «qcow2» и поддерживают создание снэпшотов.

1.1.79. ECP Veil обеспечивает:

– создание шаблонов ВМ;

– создание новых ВМ на базе снэпшотов дисков шаблона ВМ (тонкие клоны);

– создание новых ВМ на базе шаблонов.

1.1.80. ECP Veil обеспечивает возможность ограничения пропускной способности сетевого канала для различных типов трафика на прием и на передачу.

1.1.81. ECP Veil обеспечивает возможность зеркалирования сетевых портов.

1.1.82. ECP Veil обеспечивает автоматический перезапуск ВМ на резервном физическом сервере при отключении питания на основном.

1.1.83. ECP Veil обеспечивает при включенном режиме высокой доступности возможность принудительного выключения физических серверов (ограждения) при отсутствии интерфейса IPMI.

1.1.84. ECP Veil обеспечивает мониторинг доступности физических серверов через сеть управления, через интерфейс IPMI или через общее хранилище, подключенное по протоколу NFS.

1.1.85. ECP Veil обеспечивает создание учетных пользователей со следующими ролями:

– администратор ВМ;

– администратор безопасности;

– администратор сетей;

– администратор СХД;

– администратор;

– оператор;

– только для чтения.

1.1.86. ECP Veil обеспечивает возможность:

– очистки журнала событий из Web-интерфейса;

– выгрузки архивного файла журналов из Web-интерфейса.

1.1.87. ECP Veil обеспечивает вывод детальной информации о подключенных локальных устройствах хранения данных.

1.1.88. ECP Veil обеспечивает вывод информации с IPMI-датчиков сервера при их наличии.

1.1.89. ECP Veil обеспечивает возможность мониторинга по протоколу SNMP компонентов программного обеспечения:

– ресурсы системы и их использование;

– системное окружение;

– информация о ВМ;

– высокая доступность и катастрофоустойчивость ВМ.

Для мониторинга используется файл с базой управляющей информации (MIB).

1.1.90. ECP Veil позволяет:

– создавать и запускать ВМ с количеством виртуальных процессоров до 128;

– создавать и запускать ВМ с объемом оперативной памяти до 4 Тбайт;

– подключать к ВМ виртуальные диски размером до 64 Тбайт.

1.1.91. ECP Veil обеспечивает создание пулов данных с файловой системой ZFS на подключенных блочных хранилищах.

1.1.92. ECP Veil обеспечивает возможность использования одного физического сетевого интерфейса несколькими ВМ с применением технологии SR-IOV.

1.1.93. ECP Veil обеспечивает мониторинг баланса использования ресурсов в кластере и вывод предупреждений в журнал. Мониторинг выполняется на основе следующих метрик:

– загрузка центрального процессора;

– загрузка оперативной памяти;

– суммарная загрузка центрального процессора и оперативной памяти.

1.1.94. ECP Veil обеспечивает возможность автоматизированного выравнивания использования ресурсов в кластере путем перемещения ВМ между физическими серверами (автоматический режим DRS).

1.1.95. ECP Veil обеспечивает возможность сбора и вывода информации о подключенных активных сетевых устройствах с применением протокола LLDP.

1.1.96. ECP Veil обеспечивает возможность зеркалирования трафика, приходящего с сетевых интерфейсов ВМ на сетевые интерфейсы других ВМ и на сетевые интерфейсы физических серверов.

1.1.97. ECP Veil обеспечивает возможность добавления в ВМ виртуальных графических ускорителей на базе видеокарт NVidia Tesla.

1.1.98. ECP Veil обеспечивает возможность создания следующих задач по расписанию для ВМ:

– включение;

– выключение;

– принудительное выключение;

– пауза;

– перезагрузка;

– принудительная перезагрузка;

– удаление;

– резервное копирование;

– создание снэпшота;

– удаление.

1.1.99. ECP Veil обеспечивает возможность создания следующих задач по расписанию для физических серверов:

– обновление;

– резервное копирование конфигурации.

1.1.100. ECP Veil обеспечивает возможность добавления резервных физических интерфейсов в распределенный виртуальный коммутатор.

1.1.101. ECP Veil обеспечивает возможность выбора внутренних интерфейсов распределенного коммутатора при создании виртуальной сети.

1.1.102. ECP Veil обеспечивает возможность фильтрации в журнале событий по следующим полям:

– пользователю;

– отдельной сущности.

1.1.103. ECP Veil обеспечивает возможность создания задач для выполнения один раз или со следующей периодичностью:

– раз в час;

– раз в день;

– раз в неделю;

– раз в месяц.

1.2. Требования к техническим средствам

1.2.1. ECP Veil функционирует на базе средств вычислительной техники с характеристиками:

– процессор – не менее четырех ядер;

– оперативная память – не менее 8 Гбайт;

– постоянное запоминающее устройство – не менее 32 Гбайт;

– интерфейсы сетевые – не менее 1 Гбит Ethernet, в количестве не менее двух. Поддерживаются сетевые интерфейсы до 40 Гбит/с.

1.2.2. ECP Veil предназначена для использования на серверных платформах с архитектурой x86–64.

1.2.3. Аппаратные требования к физическому серверу:

– материнская (процессорная) плата и процессор должны поддерживать технологию аппаратной виртуализации – VT-d и VT-x для Intel, AMD-v для AMD или другую аналогичную технологию;

– материнская (процессорная) плата должна поддерживать установку не менее двух процессоров;

– каждый процессор должен иметь не менее четырех физических ядер и не менее восьми вычислительных потоков;

– должно быть установлено не менее двух процессоров;

– объем установленной оперативной памяти должен быть не менее 16 Гбайт;

– каждый сервер должен иметь возможность установки не менее двух накопителей на жёстком магнитном диске (НЖМД) с интерфейсом SATA/SAS;

– объем каждого установленного НЖМД должен быть не менее 500 Гбайт;

– при установке более одного НЖМД все установленные НЖМД должны быть однотипными;

– каждый сервер должен иметь выделенный аппаратный интерфейс управления IPMI;

– каждый сервер должен иметь не менее двух портов на материнской (процессорной) плате;

– каждый имеющийся в системе сетевой интерфейс (кроме IPMI) должен поддерживать технологии 1 Гбит Ethernet и Jumbo Frame;

– каждый сервер должен иметь не менее одного полноценного интерфейса PCIe x4/x8/x16 для установки дополнительного сетевого адаптера.

1.2.4. Для установки ECP Veil на физический сервер необходимо, чтобы данный сервер обладал портом или устройством в соответствии с выбранным методом установки:

– для установки с CD/DVD-диска должен быть внутренний или внешний CD/DVD-привод с возможностью загрузки с него в BIOS сервера;

– для установки с USB-накопителя должен быть USB-порт с возможностью загрузки с него в BIOS сервера;

– для установки по сети должен быть сетевой интерфейс с поддержкой загрузки по протоколу PXE и возможностью загрузки с него в BIOS сервера;

– для установки через IPMI-интерфейс должна быть поддержка подключения ISO-образа для загрузки в IPMI-интерфейсе.

1.2.5. Программные (функциональные) требования к физическому серверу:

– для работы в штатном режиме используется кластер серверов, состоящий не менее чем из трех физических серверов для среды выполнения ВМ;

– допускается эксплуатация ECP Veil в составе двух физических серверов с (без) сетью хранения данных с применением ограниченного функционала управления.

Примечание. Ограниченный функционал управления заключается в переводе в ручной режим:

– управляющих механизмов миграции ВМ;

– управляющих механизмов отказоустойчивости;

– управляющих механизмов распределения ВМ по серверам.

1.2.6. Для корректной работы ECP Veil необходимо:

– не менее одного выделенного интерфейса IPMI;

– не менее одного интерфейса 1 Гбит Ethernet;

– не менее одного интерфейса 10 Гбит Ethernet.

Примечание. Допускается использование двух интерфейсов 1 Гбит Ethernet с ограничением скорости работы операций миграции и дисковых операций ВМ, диски которых находятся на внешних (общих) хранилищах.

1.2.7. Для дисковых подсистем серверов общего назначения, применяемых для хранения данных ВМ, применяются те же требования, что и для сервисов, исполняемых внутри самих ВМ.

1.2.8. Для выбора процессоров и памяти, устанавливаемых в серверы кластера ECP Veil, необходимо учитывать, что для одной ВМ может быть выделено:

– виртуальных процессоров не более, чем имеющихся в наличии физических ядер;

– виртуальной памяти не более, чем установленной физической памяти.

1.3. Требования к программному обеспечению

1.3.1. В состав ТОС входят все компоненты, которые необходимы для корректного функционирования ECP Veil. При соблюдении требования установки или обновления программного обеспечения (ПО) только с репозиториев разработчика гарантируется корректное функционирование ECP Veil. При необходимости использования дополнительного или стороннего ПО необходимо связаться со службой технической поддержки разработчика.

1.4. Требования к квалификации специалистов

1.4.1. Специалист, производящий установку ECP Veil, должен обладать знаниями, соответствующими специализации «Администратор Linux», «Администратор сетей передачи данных» в областях:

– установка ОС Linux семейства Debian/Ubuntu;

– настройка ОС Linux семейства Debian/Ubuntu;

– настройка и эксплуатация систем на базе Linux KVM;

– основы построения сетей передачи данных TCP/IP, VLAN, настройка поддержки Jumbo Frame, ALCP, VLAN на коммутаторах.

2. СТРУКТУРА ПРОГРАММЫ

2.1. В программе реализован принцип модульного построения программного обеспечения, когда каждый отдельный модуль отвечает за решение узкоспециализированной задачи. Всё программное обеспечение разделяется на несколько подсистем. Каждая подсистема в свою очередь разделяется на набор модулей, которые реализуют определенную специализированную задачу.

2.2. Взаимодействие между модулями организовано на базе прямой адресации объектов в пределах одной подсистемы или же с использованием буферизированных средств взаимодействия (файлы, сокеты и сигналы).

2.3. В состав ECP Veil входят два программных компонента – модуль управления МК и ТОС. Структурная схема ECP Veil приведена на рис. 1.

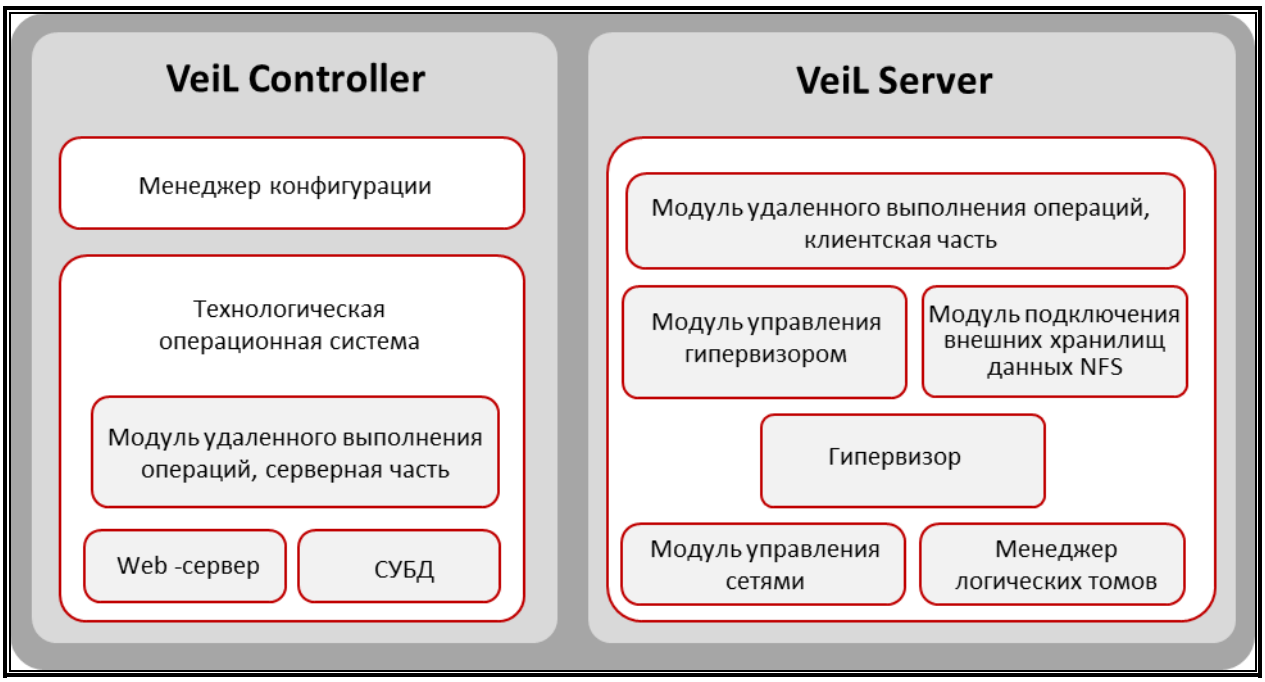

Рис. 1

2.3.1. МК представляет собой программный комплекс, предназначенный для управления ECP Veil.

В состав МК входят следующие используемые программные продукты:

– ПО, распространяемое в рамках лицензий GNU/GPL;

– ПО Apache License 2.0.

Web-интерфейс МК, RESTfull API-интерфейс и логика управления являются продуктами собственной разработки с применением интерпретаторов type-script и Python.

2.3.2. ТОС – это технологическая операционная система на базе ядра Linux 4.4. В ТОС входит комплект совместимых (проверенных) версий ПО, необходимый для корректного функционирования ECP Veil. Обновление ПО в составе ТОС может проводиться только с использованием репозиториев разработчика. Обновления из других источников не допускаются, иначе исполнитель (разработчик) не несет ответственности за ущерб, нанесенный данным клиента.

Примечание. При соблюдении требования установки или обновления ПО только с репозиториев разработчика гарантируется корректное функционирование ECP Veil. При необходимости использования дополнительного или стороннего ПО необходимо связаться с технической поддержкой разработчика.

2.4. Для установки модулей ECP Veil не требуется отдельной установки базовой ОС общего назначения. Установка модулей производится с дистрибутива непосредственно на физический сервер без предварительной установки дополнительного ПО.

2.5. Запуск ВМ обеспечивается модулем-гипервизором qemu-kvm, входящим в состав ТОС. Гипервизор qemu-kvm устанавливается непосредственно на физический сервер вместе с ТОС с дистрибутива ECP Veil и отдельной установки не требует.

3. НАСТРОЙКА ПРОГРАММЫ

3.1. Общие сведения

3.1.1. Для установки программы на серверную платформу к ней должны быть подключены следующие устройства:

– технологический монитор;

– клавиатура;

– технологический дисковод DVD-ROM.

3.1.2. Если серверная платформа не имеет возможности подключения монитора и клавиатуры, то необходимо обеспечить доступ по протоколу IPMI или доступ к Web-интерфейсу управления IPMI модуля по сети.

Примечание. Перед установкой программы на серверную платформу должны быть установлены сетевые карты в соответствии с конструкторской документацией.

3.2. Проверка целостности программы

3.2.1. Непосредственно перед установкой должна быть проверена контрольная сумма установочного компакт-диска ИСКП.00021-01. Проверка контрольной суммы осуществляется на ЭВМ, на которую установлена ОС «Debian» версии 10.4.0.

3.2.2. Для проверки контрольной суммы установочного диска необходимо выполнить следующую последовательность действий:

– войти в ОС под учетной записью суперпользователя (учетная запись «root») и дождаться приглашения ввода консоли;

– вставить компакт-диск ИСКП.00021-01 в дисковод DVD-ROM;

– смонтировать компакт-диск с помощью команды

mount␣/dev/sr0 /mnt/cdrom

– перейти в каталог точки монтирования компакт-диска (каталог с содержимым компакт-диска) с помощью команды

cd␣/mnt/cdrom

Примечание. Каталог точки монтирования компакт-диска зависит от настроек рабочего места и может отличаться;

– в командной строке набрать команду для подсчета контрольной суммы

find␣.␣-type␣f␣-exec␣md5sum␣{}␣\;␣|␣sort␣-k2␣|␣md5sum

Примечание. Будьте внимательны при наборе команды. От правильности набора будет зависеть результат;

– дождаться окончания выполнения введенной команды и получить на мониторе подсчитанную контрольную сумму;

– размонтировать компакт-диск с помощью команды

cd␣/;␣umount␣/dev/sr0

– извлечь компакт-диск ИСКП.00021-01 из дисковода DVD-ROM.

3.2.3. Программа считается готовой к установке, если контрольная сумма, отображенная на мониторе ЭВМ для компакт-диска ИСКП.00021-01, совпала с контрольной суммой этого диска, записанной в формуляре ИСКП.00021-01 30 01.

Примечание. При несовпадении контрольных сумм запрещается производить дальнейшие действия по установке программы.

3.3. Установка программы

3.3.1. Подготовка к работе

3.3.1.1. Перед началом работы необходимо выполнить следующие действия:

– убедиться, что всё оборудование комплектно, исправно и соответствует минимальным требованиям. Если в состав кластера виртуализации будет входить оборудование, не входящее в комплект поставки, его также надо подготовить до начала развёртывания кластера;

– при развёртывании кластера в рамках уже существующей инфраструктуры необходимо заранее собрать информацию, требуемую для корректной интеграции ECP Veil в инфраструктуру. Для оценки объёма необходимой информации перед началом развёртывания необходимо ознакомиться с данным руководством;

– для корректной работы ECP Veil необходимо на всех серверах кластера настроить IPMI-интерфейсы таким образом, чтобы они находились в одной подсети. Использование данной подсети для других целей, в том числе в рамках ECP Veil, не допускается.

Примечания:

1. При наличии собственной системы мониторинга и управления по IPMI необходимо учитывать, что управление серверами кластера другими средствами (не самого кластера) по данному протоколу может нарушить его работу.

В данном случае исполнитель (разработчик) не несет ответственности за ущерб, нанесенный данным клиента.

2. В общей сложности в рамках ECP Veil будет функционировать четыре служебные, частично или полностью, изолированные сети. При настройке ECP Veil необходимо учитывать, что данные сети не смогут быть использованы для других целей в дальнейшем, так как система управления ECP Veil не позволит их инициализировать, а принудительная (ручная) настройка их может вызвать отказы в работе или снижение производительности системы.

3. Возможна установка ECP Veil в роли «Node» на ВМ, работающие в средах ECP Veil, VMware, Oracle Virtualbox, Microsoft Hyper-V, RHEV и других без ограничений.

4. Возможна установка ECP Veil в роли «Controller+Node» на ВМ, работающие в средах ECP Veil, VMware ESXi, Oracle Virtualbox, Microsoft Hyper-V, RHEV и других без ограничений.

5. Возможна загрузка образа ВМ с предустановленным ECP Veil в роли «Controller+Node» с официального сайта *https://veil.mashtab.org* по запросу.

3.3.2. Предварительная настройка оборудования

3.3.2.1. Для предварительной настройки необходимо выполнить следующие действия:

– подключить оборудование к электропитанию и сетям передачи данных;

– включая серверы, поочередно произвести настройку IPMI-интерфейсов в BIOS.

ВНИМАНИЕ! Рекомендуется выдавать адреса таким образом, чтобы по ним было легко идентифицировать серверы в составе кластера. Это упростит последующую настройку ECP Veil и дальнейшее обслуживание оборудования;

– настроить серверы таким образом, чтобы имелась возможность установки ТОС с носителя;

– убедиться, что НЖМД не имеют разметки или режим установки UEFI/LEGACY выбран в соответствии с имеющейся разметкой диска;

– при наличии в составе сервера устройств, требующих специализированных драйверов, подготовить носитель с драйверами;

– убедиться, что сервер подключен по Ethernet к сети, подключенной к DHCP-серверу.

3.3.3. Установка с физического носителя

3.3.3.1. Для установки с CD/DVD выполнить:

– вставить компакт-диск ИСКП.00021-01 в дисковод CD/DVD-ROM;

– при загрузке сервера активировать опцию «Boot menu»;

– при появлении меню выбрать из списка необходимый привод CD/DVD;

– если пункт загрузки с CD/DVD не обнаружен, зайти в BIOS, используя опцию «BIOS Setup» (в этом же меню или при перезагрузке), и убедиться, что опция загрузки с CD/DVD активирована и необходимый привод CD/DVD есть в списке доступных устройств;

– после отображения на экране монитора выбора типа установки перейти к 3.3.5 «Процедура установки ECP Veil» данного руководства.

3.3.3.2. Для установки с USB-накопителя выполнить:

– установить USB-накопитель в разъем USB (желательно находящийся на задней панели сервера);

– при загрузке сервера активировать опцию «Boot menu»;

– при появлении меню выбрать из списка необходимый USB-накопитель;

– если пункт загрузки с USB-накопителя не обнаружен, зайти в BIOS, используя опцию «BIOS Setup» (в этом же меню или при перезагрузке), и убедиться, что опция загрузки с USB-накопителя активирована и необходимый USB-накопитель есть в списке доступных устройств;

– после отображения на экране монитора выбора типа установки перейти к 3.3.5 «Процедура установки ECP Veil» данного руководства.

3.3.3.3. Для установки по сети выполнить:

– подготовить собственный источник установки по PXE (Preboot Execution Environment) и разместить в нем данные с носителя ECP Veil в соответствии с инструкцией по настройке ОС, установленной на сервере сетевой установки;

– для установки с PXE при загрузке сервера активировать опцию «Boot menu»;

– при появлении меню выбрать из списка необходимый сетевой интерфейс, подключенный к сети с настроенным сервисом PXE установки;

– если пункт загрузки по сети не обнаружен, зайти в BIOS, используя опции «BIOS Setup» (в этом же меню или при перезагрузке), и убедиться, что опция загрузки по сети (с PXE) активирована и необходимый сетевой интерфейс есть в списке доступных устройств;

– при установке средствами, предоставляемыми интерфейсом управления IPMI, действовать в соответствии с инструкциями к данному интерфейсу (предоставляются производителем оборудования);

– после отображения на экране монитора выбора типа установки перейти к 3.3.5 «Процедура установки ECP Veil» данного руководства.

3.3.4. Миграция с другой платформы виртуализации на базе Linux KVM

3.3.4.1. Данная операция требует достаточной квалификации сотрудников в области администрирования ECP Veil и Linux based ОС, задействованных в исполнении данной процедуры.

Для миграции на ECP Veil с другой платформы виртуализации необходимо:

– освободить один из серверов в составе старого кластера или взять один новый сервер и развернуть на нем ECP Veil;

– используя общее хранилище, выполнить перенос данных ВМ, подготовленных к экспорту, в ECP Veil.

Примечание. ECP Veil поддерживает импорт qcow2 и img-образов, а также конвертацию OVF/OVA в qcow2/img для импорта.

3.3.5. Процедура установки ECP Veil

Установка ECP Veil проходит в два этапа:

– установка контроллера (Controller + Node);

– установка сервера виртуализации (Node).

3.3.5.1. Установка контроллера

3.3.5.1.1. Установка контроллера выполняется в следующем порядке:

1) выполнить действия, описанные в 3.3.3;

2) дождаться появления меню установки (рис. 2), выбрать установку «Install Controller + Node» и нажать «Enter»;

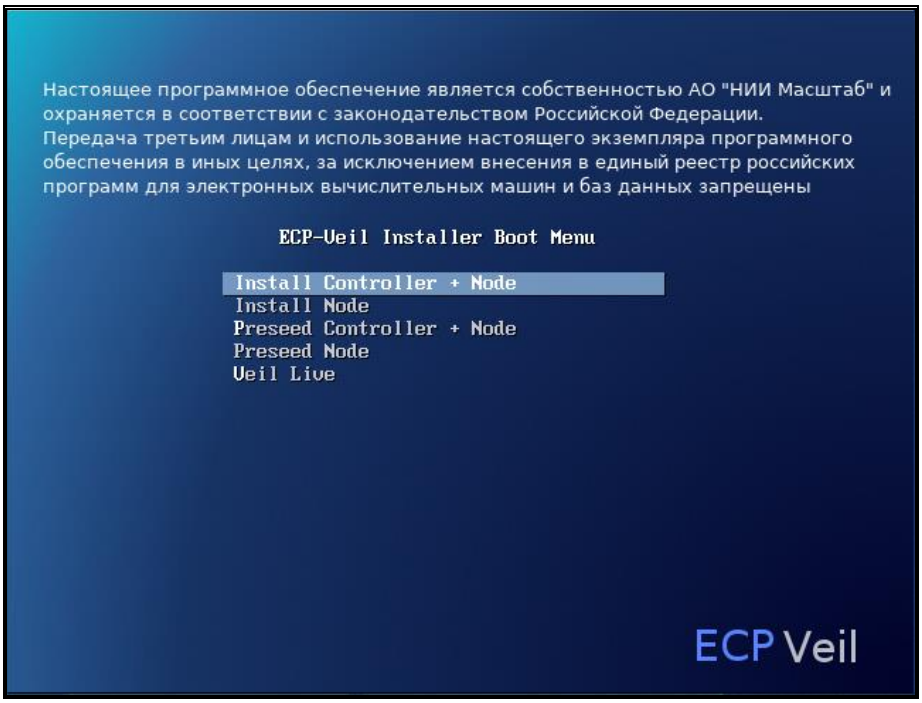

Рис. 2

3) в меню конфигурации сети выбрать необходимый сетевой интерфейс (рис. 3), через который будет проходить подключение к сети с DHCP-сервером, и нажать «Enter»;

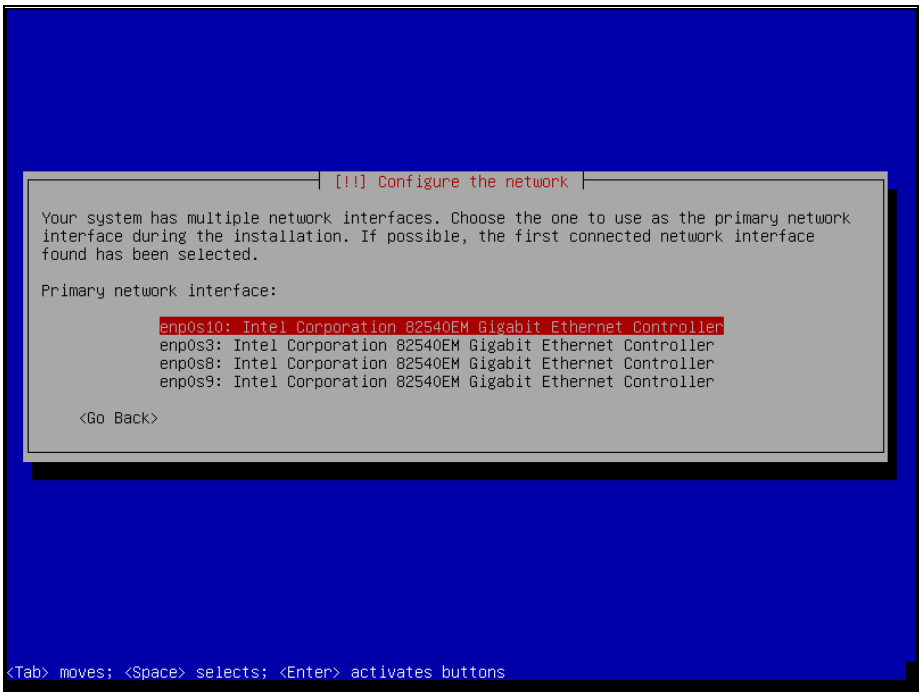

Рис. 3

4) дождаться окончания подготовки к установке (рис. 4);

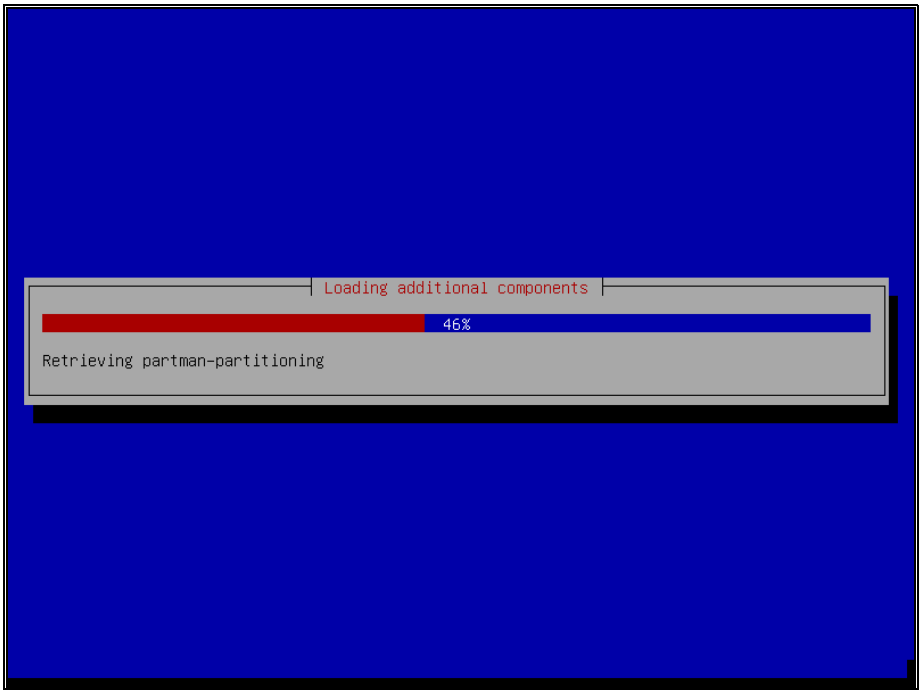

Рис. 4

5) в меню конфигурации сети задать имя хоста (рис. 5) и нажать «<Continue>»;

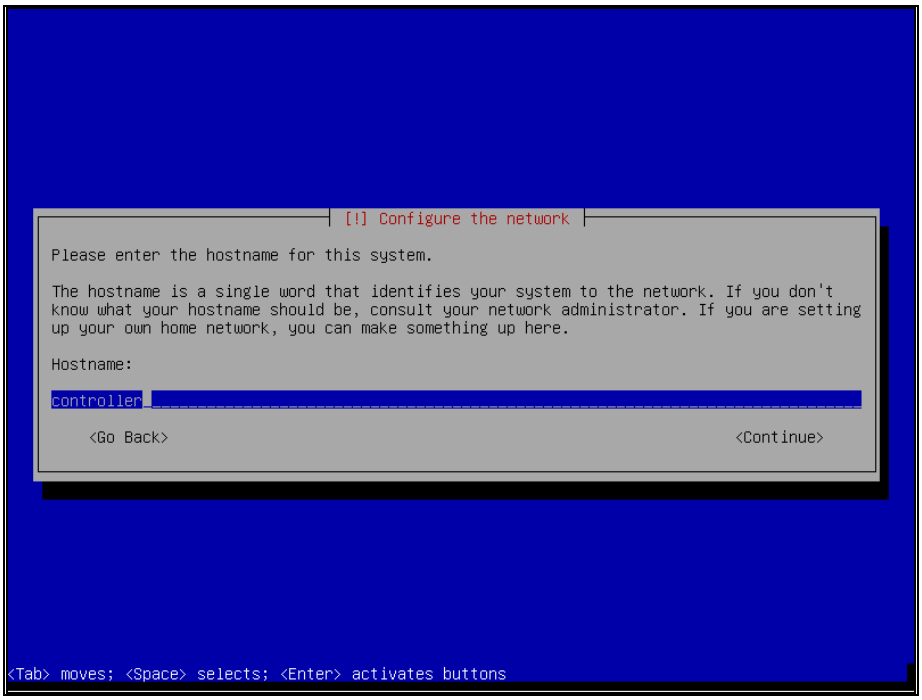

Рис. 5

6) в меню конфигурации сети задать имя домена (рис. 6) и нажать «<Continue>».

Примечание. Параметр «Domain name» может остаться пустым;

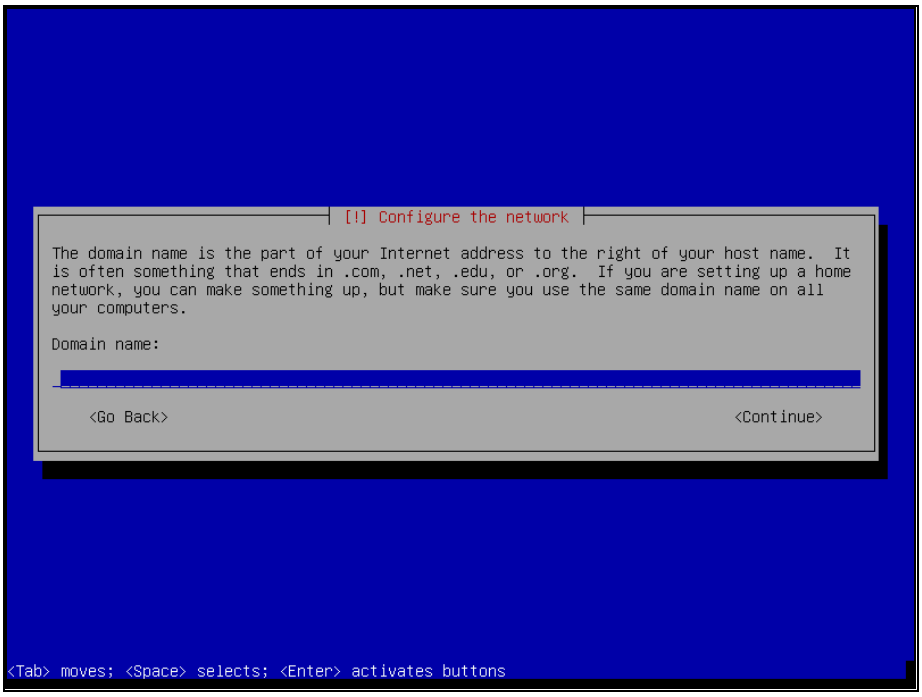

Рис. 6

7) в меню задания пользователей и паролей задать пароль для пользователя «root» (рис. 7) и нажать «<Continue>»;

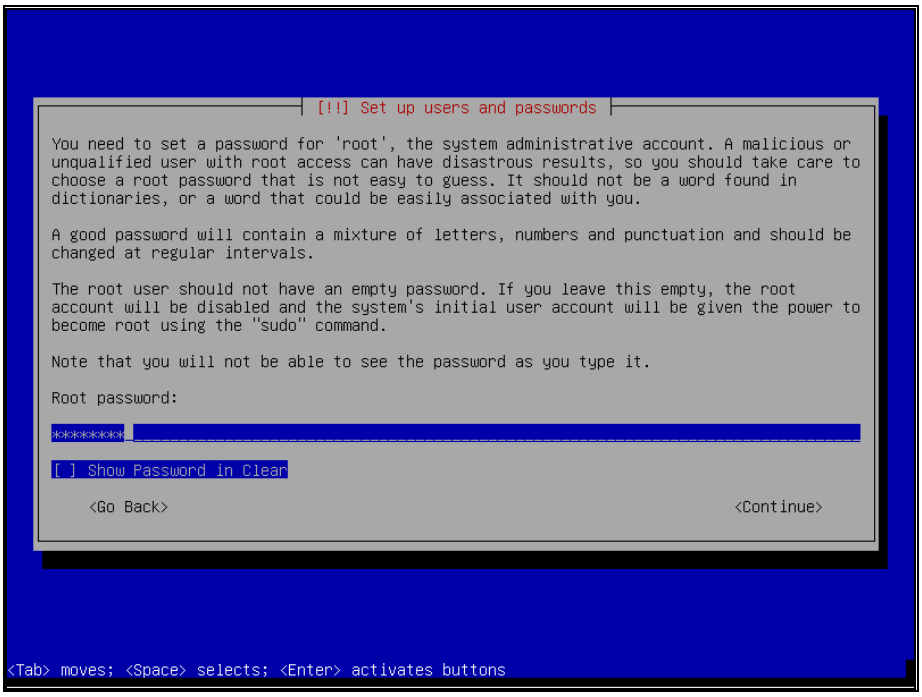

Рис. 7

8) в меню задания пользователя и пароля повторно ввести заданный на предыдущем шаге пароль для пользователя «root» (рис. 8) и нажать «<Continue>»;

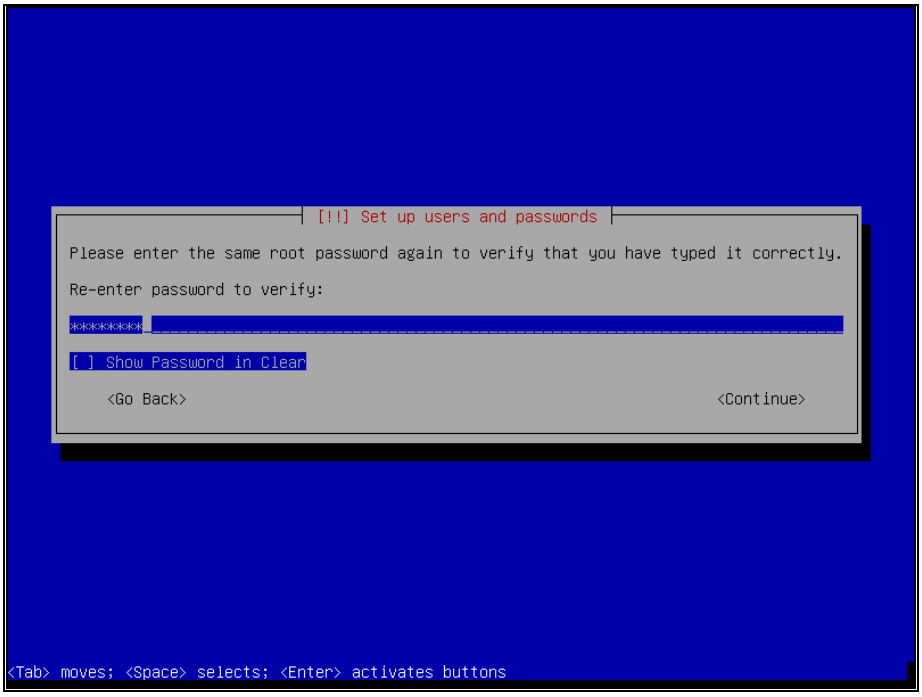

Рис. 8

9) в меню выбора временной зоны задать временную зону (рис. 9) и нажать «Enter»;

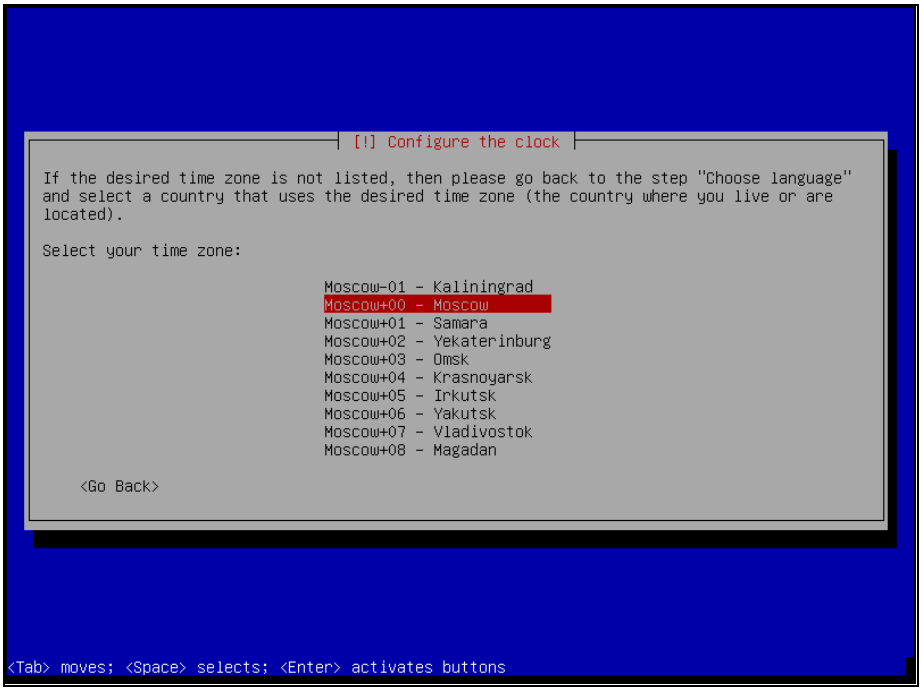

Рис. 9

10) перед разбивкой диска необходимо оценить возможности дисковой подсистемы сервера и сопоставить их с планом развёртывания.

Необходимо учитывать следующие рекомендации:

– если объём оперативной памяти сервера составляет не менее половины имеющегося дискового пространства, то использование автоматической разбивки не допускается;

– если планируется использовать внешнюю СХД для хранения образов ISO, дисков ВМ, снимков ВМ и резервных копий ВМ, то нет необходимости выделять отдельный раздел для локального хранилища на сервере;

– если предполагается использование локального хранилища сервера, то его рекомендуется монтировать в выделенный раздел;

– для управления дисковым пространством рекомендуется использовать LVM. Это связано с тем, что система управления дисковой подсистемой в ECP Veil основана на использовании LVM;

– для размещения корневой файловой системы без создания отдельного раздела для журналов системных событий (логов) рекомендуется сформировать раздел объёмом не менее 64 Гбайт;

– при использовании отдельного раздела, монтируемого в директорию без кавычек «/var/log», рекомендуется сформировать раздел объёмом не менее 32 Гбайт;

– раздел для локального хранилища данных ВМ монтируется в директорию без кавычек «/storages/local»;

– раздел подкачки (swap) рекомендуется задавать объемом не менее установленного значения оперативной памяти, но не более двух объёмов оперативного запоминающего устройства (ОЗУ);

11) далее при появлении окна выбора диска следует выбрать диск, который будет использоваться в качестве загрузочного и нажать «Enter» (рис. 10).

Если дисков несколько, то рекомендуется использовать первый в списке.

Если первым в списке диском является «LUN», предоставляемый по Fiber Channel или аппаратному iSCSI, то необходимо выбрать первый локальный диск (в случае, если установка на LUN не планировалась);

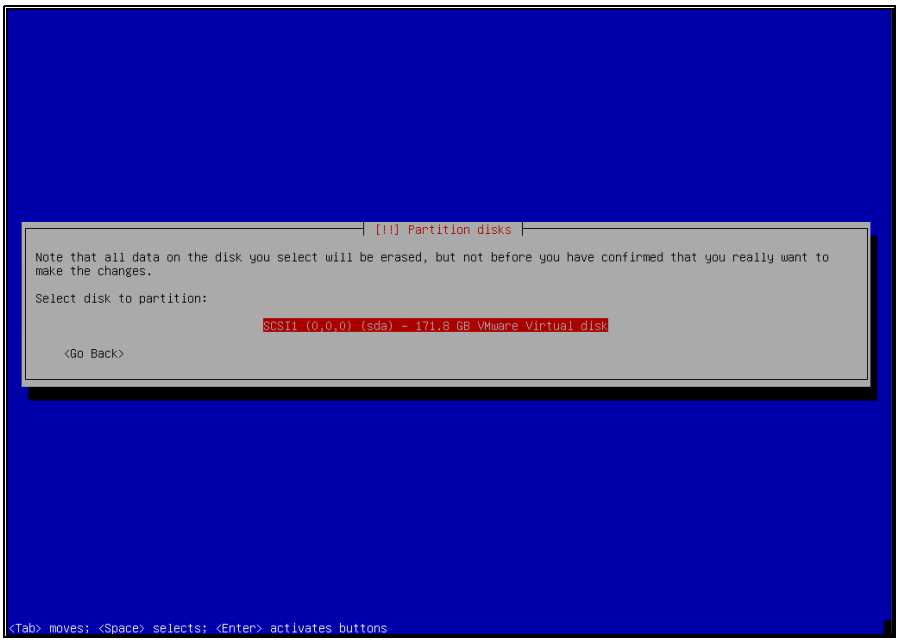

Рис. 10

12) при появлении окна предупреждения о том, что размер основного раздела в рецепте меньше объёма диска, необходимо выбрать объём в соответствии с планом развёртывания. Заданный рецептом объём основного (root) раздела (26.7 Гбайт) является минимально допустимым для развёртывания ECP Veil, рекомендованный – 100 Гбайт или равный объёму диска, если локальное хранилище не требуется (рис. 11);

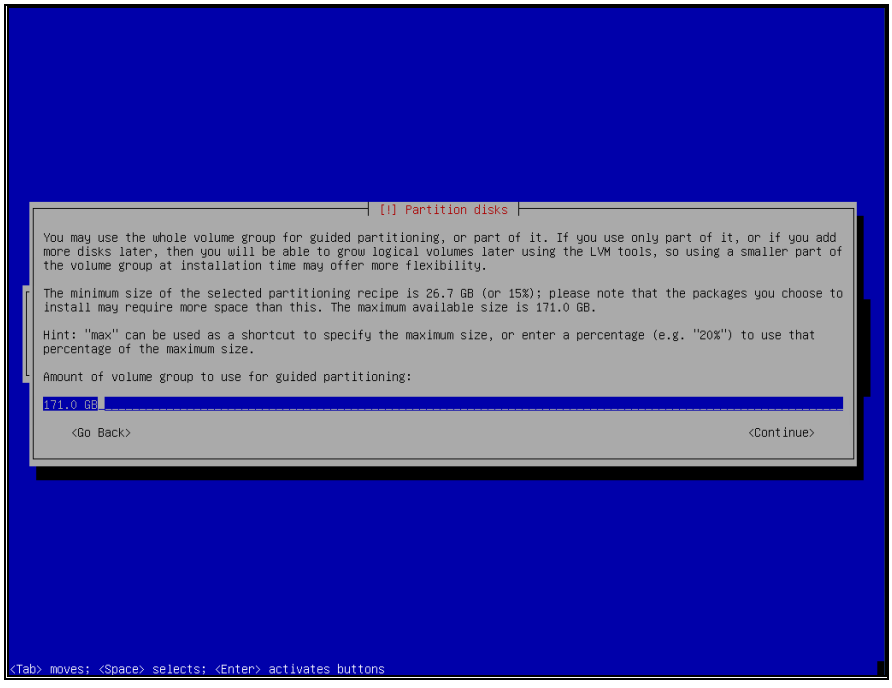

Рис. 11

13) после этого следует создать логический раздел для локального хранилища.

Примечание. Если этого не требуется, то сразу перейти к шагу 27).

Для создания локального хранилища необходимо перейти в раздел конфигурирования LVM – «Configure the Logical Volume Manager» и нажать «Enter» (рис. 12);

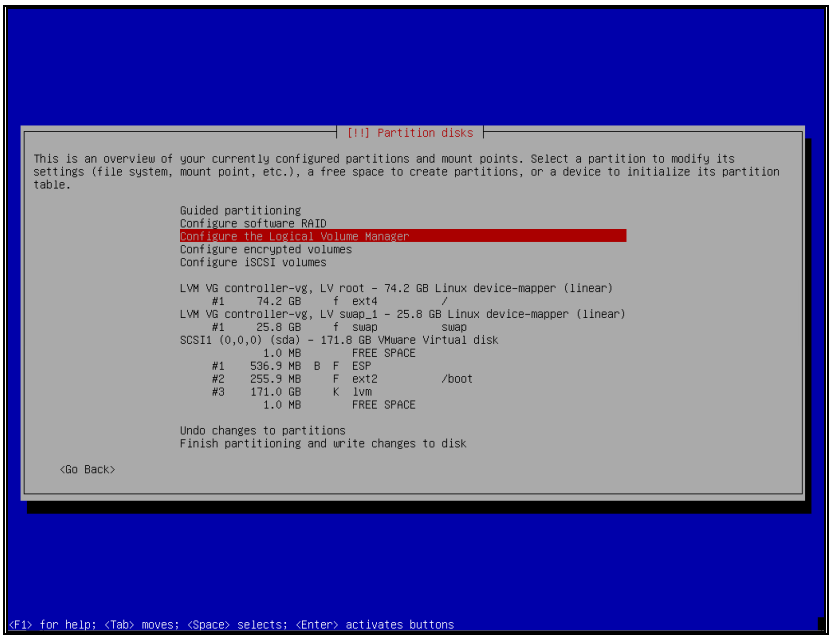

Рис. 12

14) далее следует подтвердить запись изменений на диск, нажав «<Yes>» (рис. 13);

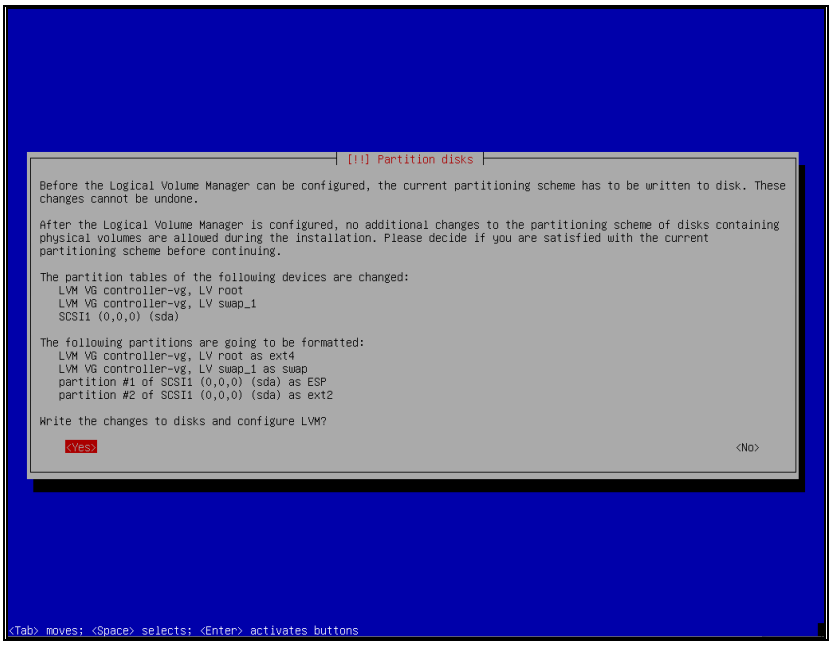

Рис. 13

15) после этого следует создать логический раздел, выбрав «Create logical volume» и нажав «Enter» (рис. 14);

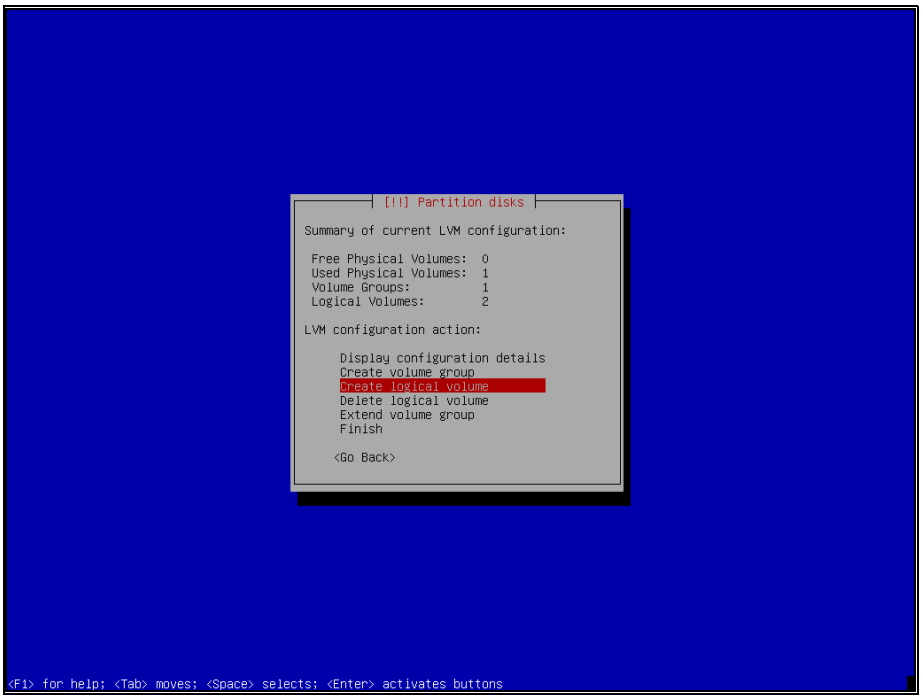

Рис. 14

16) далее следует выбрать группу логических томов, в которой создается логический том (рис. 15);

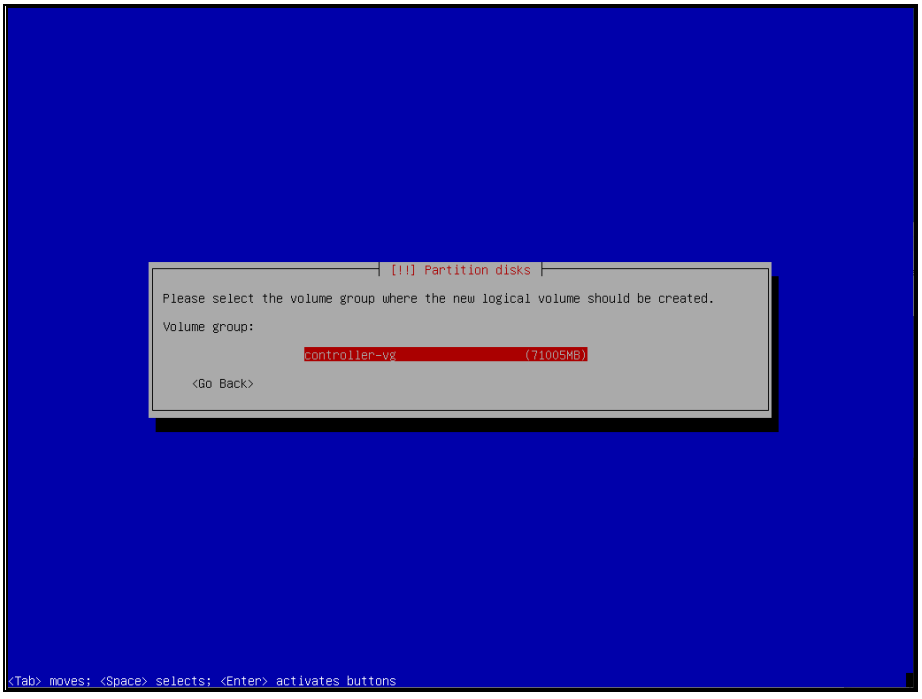

Рис. 15

17) после этого следует указать имя логического раздела (рис. 16). Затем выбрать «Continue» и нажать «Enter».

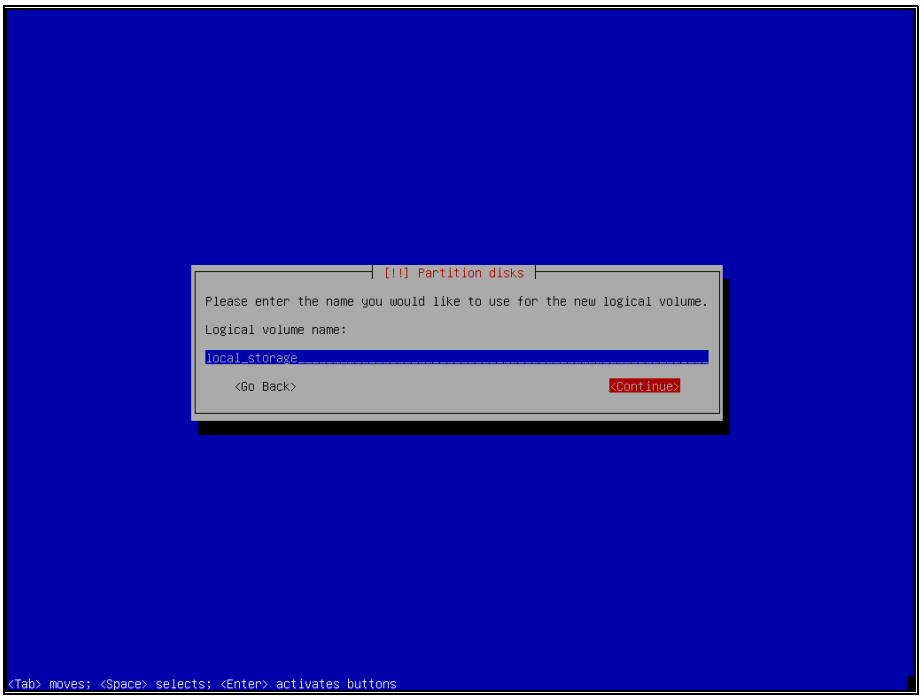

Рис. 16

В открывшемся окне необходимо указать размер раздела (рис. 17). «По умолчанию» подставляется количество свободного места в группе. Затем необходимо выбрать «Continue» и нажать «Enter».

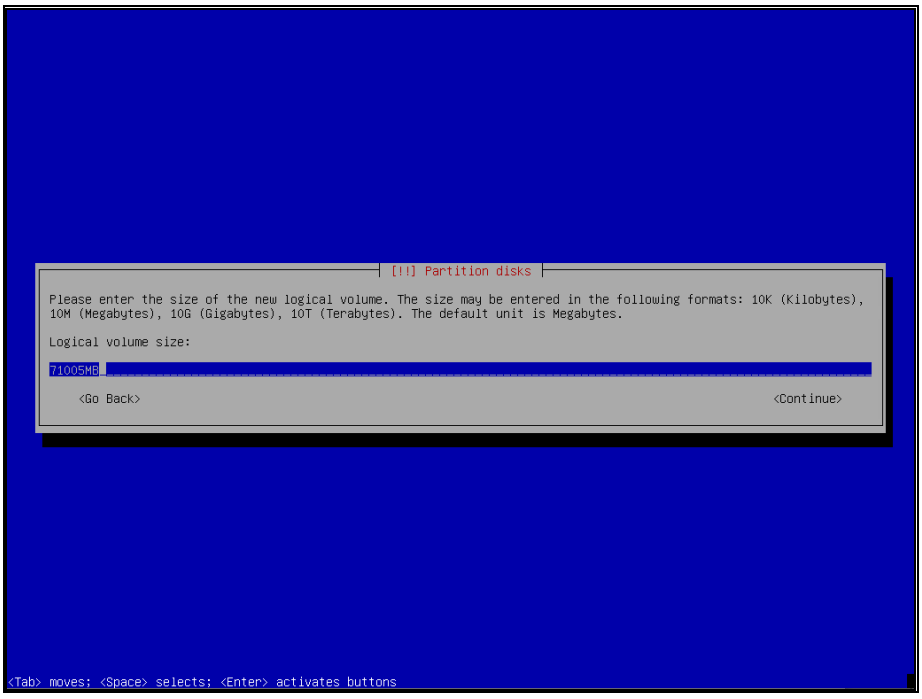

Рис. 17

Допускается выделение раздела для хранения системных логов (журналов) ОС. Отдельный раздел для журналов создается также, как и для локального хранилища. Для этого на этапе создания раздела для локального хранилища необходимо оставить свободным запланированное количество места и создать в нем логический раздел для системных журналов;

18) для проверки корректности конфигурации необходимо выбрать пункт «Display configuration details» (см. рис. 14). В открывшемся окне необходимо проверить заданную конфигурацию и нажать «<Continue>» (рис. 18);

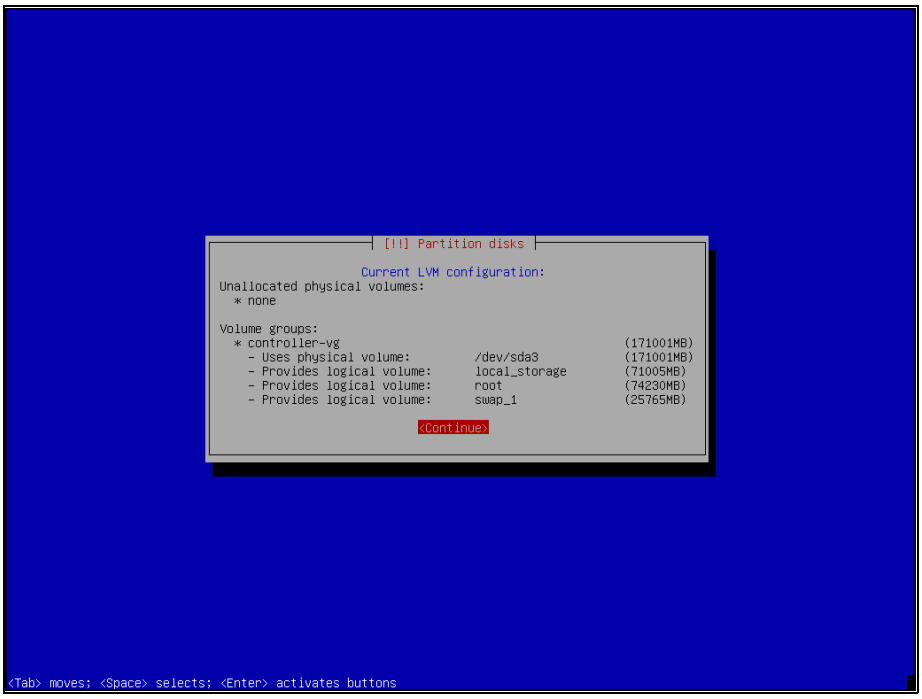

Рис. 18

19) для завершения конфигурирования дисковой подсистемы необходимо выбрать пункт «Finish» (рис. 19) и нажать «Enter»;

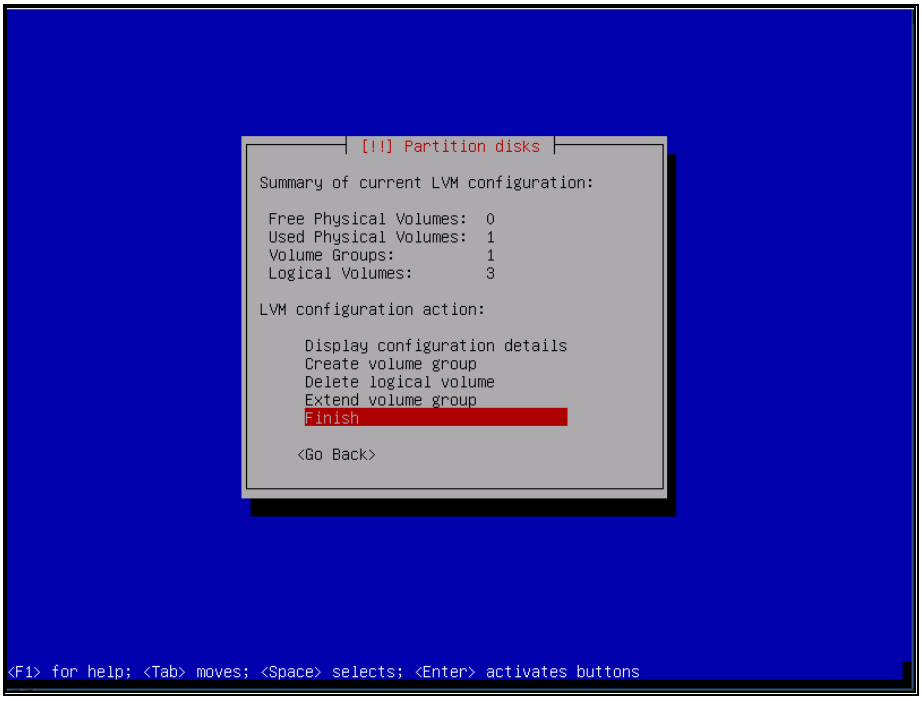

Рис. 19

20) далее следует выбрать точки монтирования для созданных разделов LVM. Для этого необходимо навести курсор на выбранный раздел и нажать «Enter» (рис. 20);

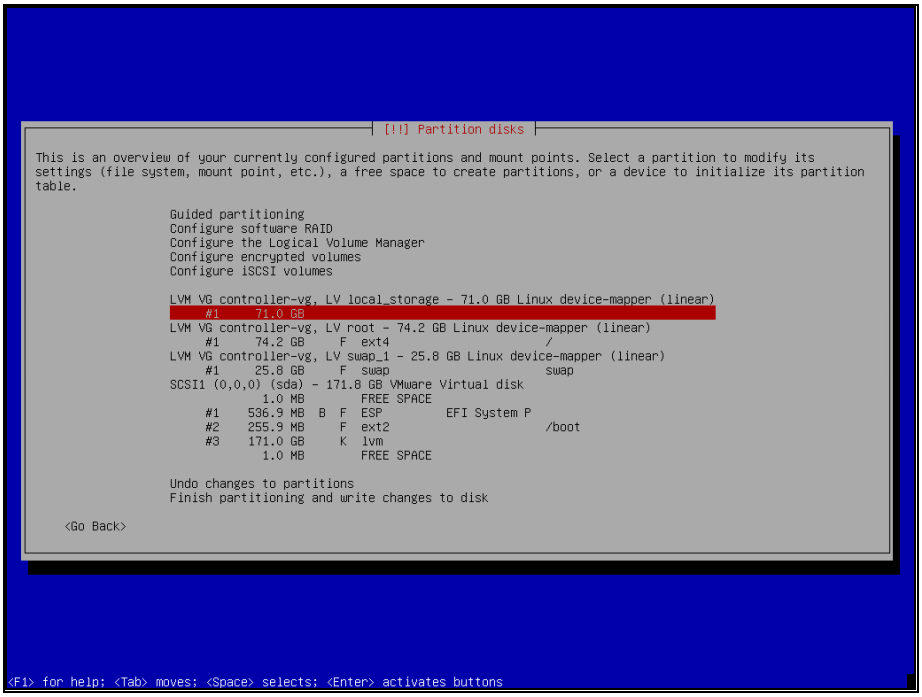

Рис. 20

21) после этого следует выбрать действия с разделом диска «Use as: do not use» и нажать «Enter» (рис. 21);

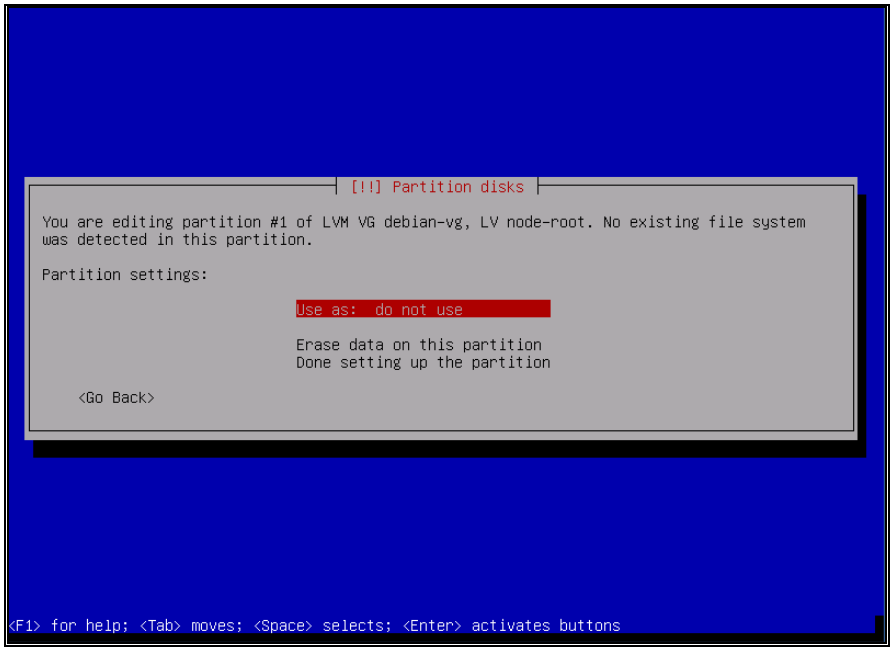

Рис. 21

22) далее следует выбрать вариант использования раздела диска «Ext4 journaling file system». Для подтверждения выбора нажать «Enter» (рис. 22);

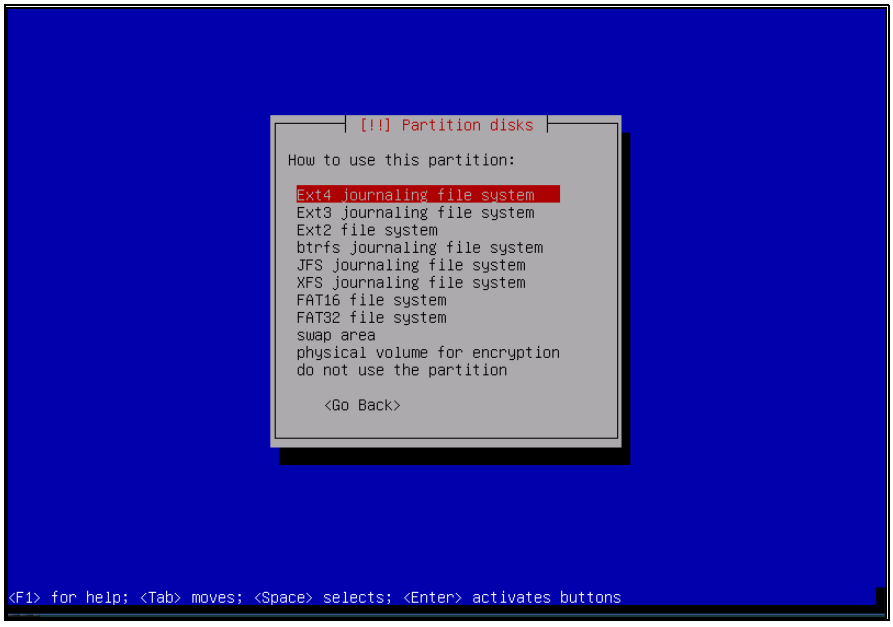

Рис. 22

23) далее следует выбрать пункт «Mount point» и нажать «Enter» (рис. 23);

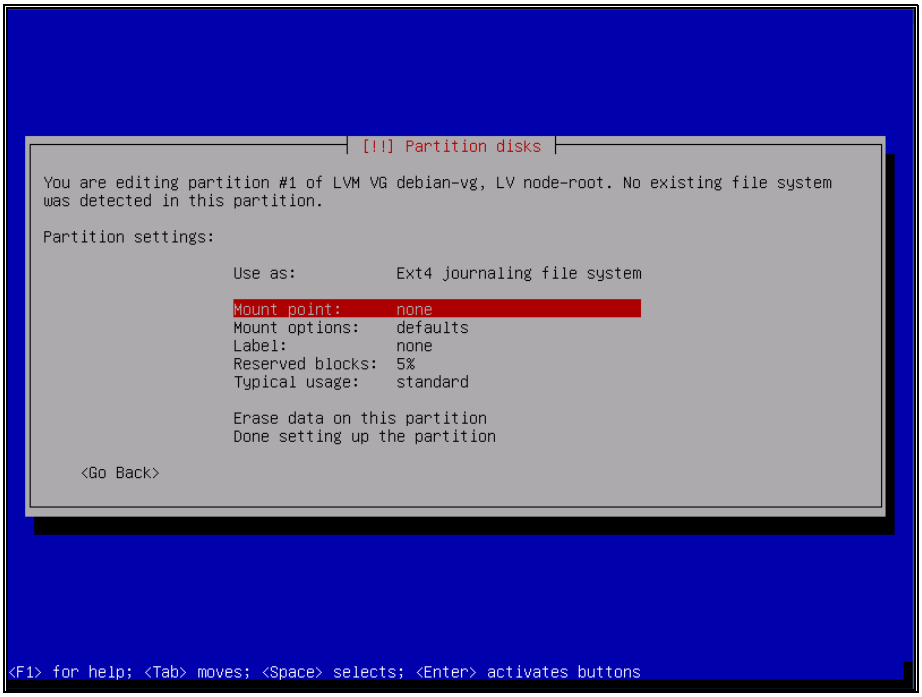

Рис. 23

24) после этого в открывшемся окне необходимо в качестве точки монтирования выбрать «Enter manually» – для локального хранилища данных ВМ. Затем задать значение «/storages/local».

Для подтверждения выбора нажать «Enter» (рис. 24);

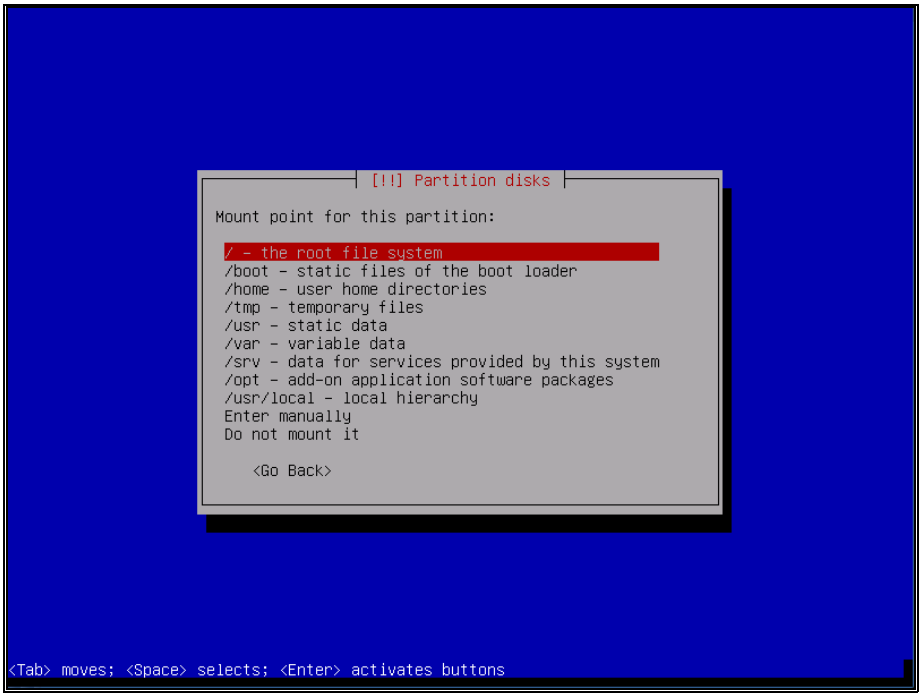

Рис. 24

25) далее в открывшемся окне следует выбрать пункт «Done setting up the partition» и нажать «Enter» (рис. 25);

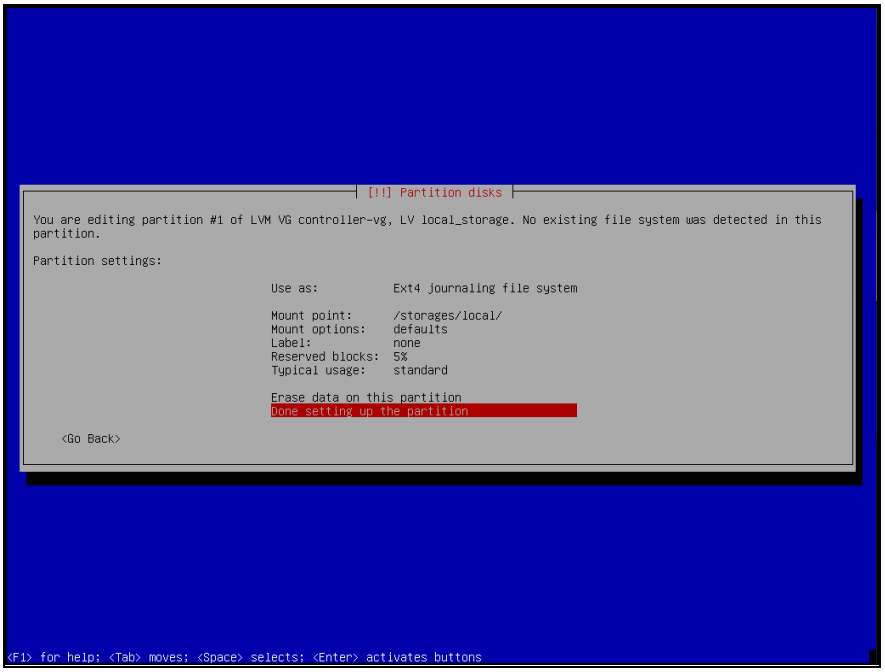

Рис. 25

26) если создавался раздел для системных журналов, то после этого в открывшемся окне необходимо выбрать следующий по списку раздел (рис. 26) и провести настройки аналогично шагам 21) – 25), выбрав в качестве точки монтирования «/var/log»;

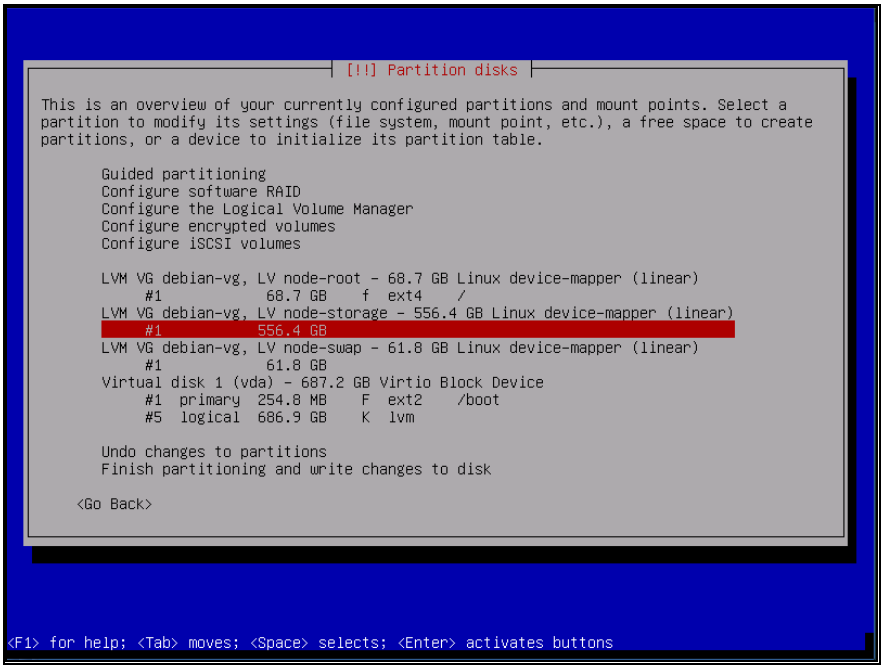

Рис. 26

27) после этого таблица разделов должна выглядеть аналогично рис. 27. Далее следует выбрать пункт «Finish partitioning and write changes to disk» и нажать «Enter»;

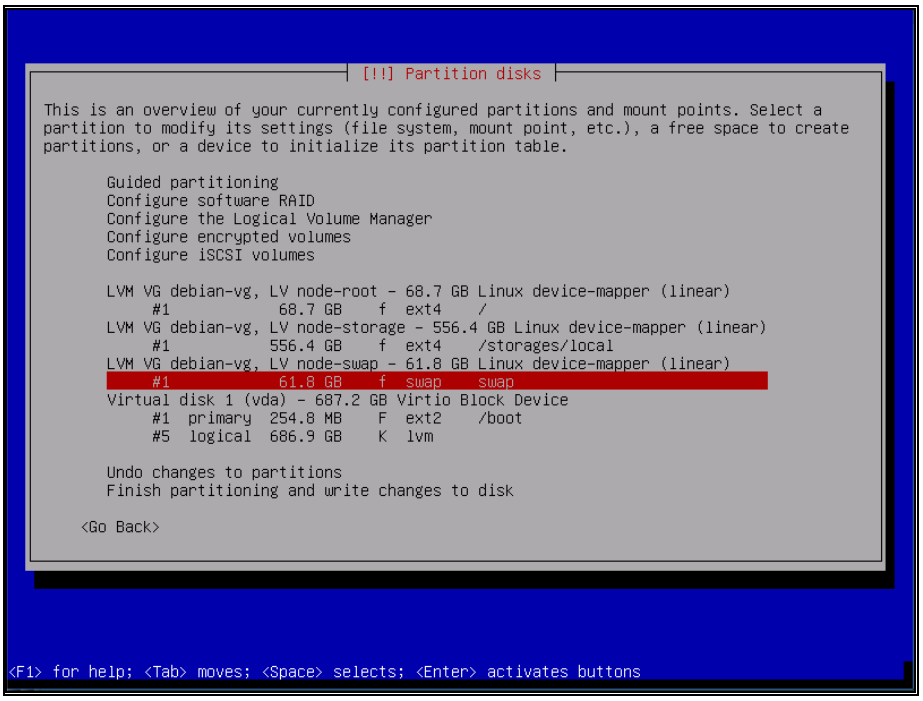

Рис. 27

28) после этого необходимо подтвердить запись изменений на диск (рис. 28);

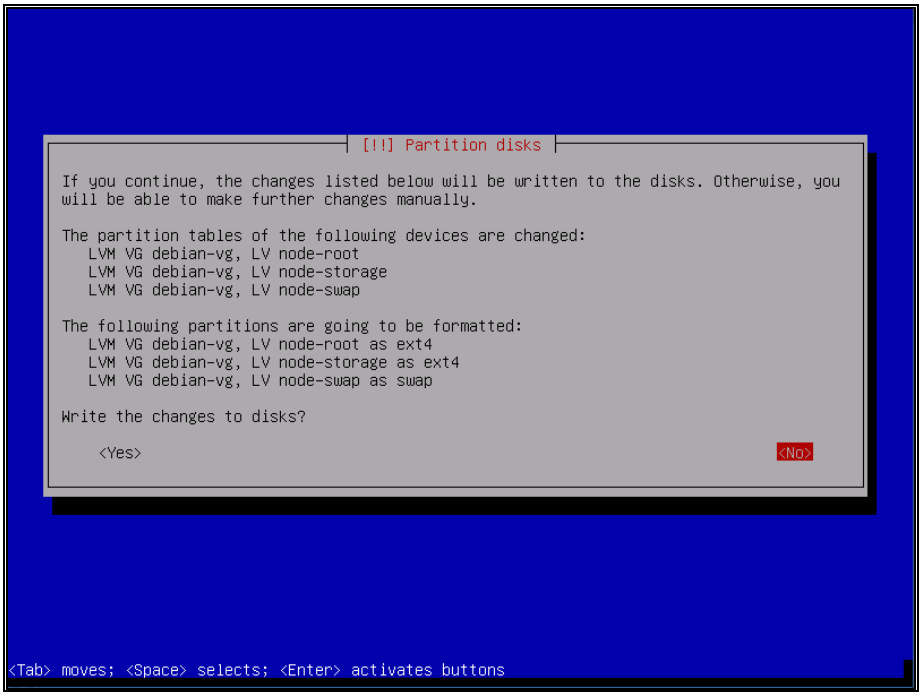

Рис. 28

29) после этого начнется установка ОС на диск (рис. 29).

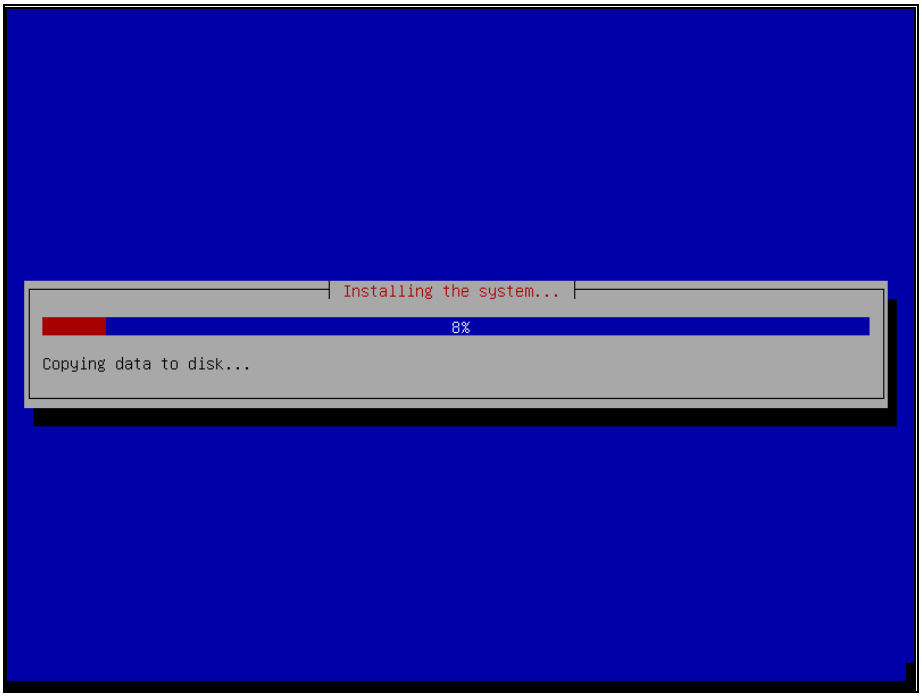

Рис. 29

Если этого не произошло и отобразилась ошибка о невозможности записи на диск, то это означает, что таблица разделов данного диска не соответствует типу загрузки сервера. Для режима загрузки «Legacy» автоматически создается таблица разделов MBR, а для UEFI – GPT. Необходимо очистить заголовок диска, перейдя в консоль для ввода команд нажатием комбинации «Alt+F4». В этой консоли необходимо выполните команду

dd if=/dev/zero of=/dev/sda bs=512 count=1000

где /dev/sda – имя диска, выбранного для установки на шаге 11). После этого необходимо начать установку сначала;

30) после окончания установки пакетной базы необходимо выбрать диск для установки загрузчика GRUB (рис. 30) – выбрать тот диск, на который была установлена ОС;

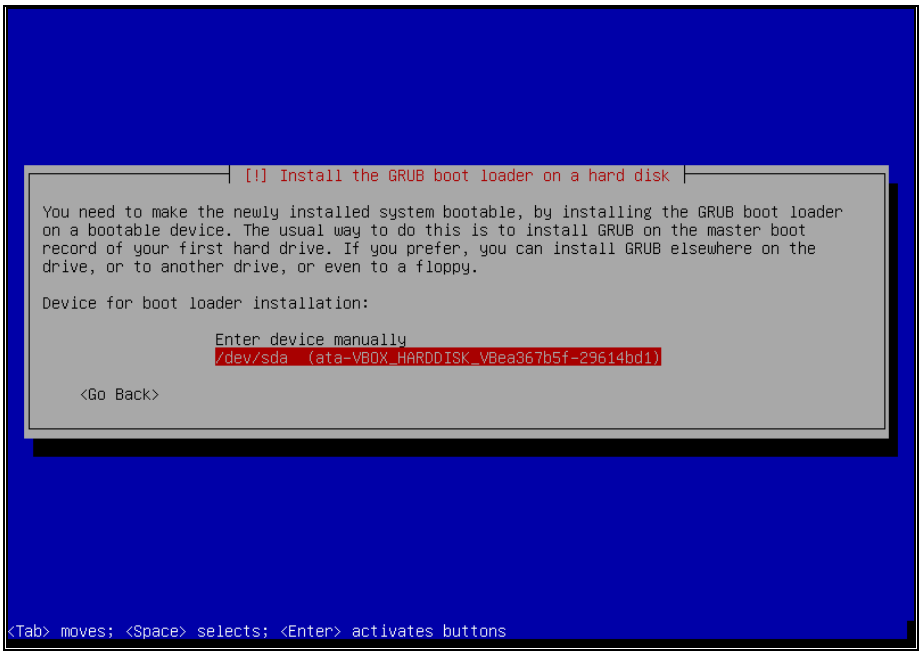

Рис. 30

31) после окончания установки аппаратная платформа автоматически перезагрузится и начнется процесс первоначальной настройки (подготовки системы к работе). После окончания настройки система ещё раз перезагрузится.

После перезагрузки аппаратной платформы для доступа к CLI-интерфейсу управления необходимо ввести имя пользователя «root» и пароль, заданный при установке сервера (рис. 31).

Рис. 31

ВНИМАНИЕ! Для подключения к сети управления (СУ) ECP Veil используется виртуальный сетевой адаптер. Для обеспечения доступа к СУ ECP Veil используется выбранный при установке или первый физический сетевой интерфейс в системе, который подключается к виртуальному коммутатору. Данный физический интерфейс должен быть подключен к СУ ECP Veil до начала установки ПО.

3.3.5.2. Базовая настройка контроллера

3.3.5.2.1. При соблюдении условий корректной установки дополнительная настройка не требуется. При необходимости проверить настройки или произвести настройку дополнительных параметров обратитесь к 3.3.5.5 данного руководства.

3.3.5.3. Установка сервера виртуализации

3.3.5.3.1. Установка сервера виртуализации выполняется в следующем порядке:

– выполнить действия, перечисленные в 3.3.3 данного руководства;

– дождаться появления меню установки (см. рис. 2), выбрать установку «Install Node» и нажать «Enter»;

– далее необходимо выполнить действия, описанные в 3.3.5.1.1 данного руководства, начиная с шага 3).

3.3.5.4. Базовая настройка сервера

3.3.5.4.1. При соблюдении условий корректной установки дополнительная настройка не требуется. При необходимости проверить настройки или произвести настройку дополнительных параметров обратитесь к 3.3.5.5 данного руководства.

3.3.5.5. Изменение сетевых параметров из консоли сервера

3.3.5.5.1. Для проверки сетевых настроек сервера, необходимых для сборки кластера, надо подключиться к консоли сервера и авторизоваться пользователю с учетной записью «root» и паролем, который был задан при установке ПО.

После авторизации в консоли пользователю будет предоставлен доступ в CLI-интерфейс.

3.3.5.5.2. Для команд агрегации доступно расширенное описание по ключу «–h». Для управления СУ ECP Veil надо использовать имя коммутатора «veil-default». Перечисление физических интерфейсов, объединяемых агрегацией, производится через пробел.

3.3.5.5.3. Для всех команд в интерфейсе CLI доступны подсказки. Для использования автоматического дополнения команд необходимо использовать на клавиатуре клавишу «Tab», а для получения подсказки необходимо выполнить команду без аргументов или с ключем «–h». Более подробное описание команд в интерфейсе CLI приведено в приложении к данному руководству.

3.3.5.5.4. Для проверки настроек сетевой подсистемы используется команда

 # net info

Данная команда возвращает настройки виртуального сетевого интерфейса управления «veil-mgmt» и необходимые настройки физических интерфейсов. На основании полученной информации можно определить, был ли выдан IP-адрес интерфейсу «veil-mgmt» или нет, и какой физический интерфейс подключен в коммутатор СУ ECP Veil «veil-default».

3.3.5.5.5. Для изменения физического интерфейса, подключенного к коммутатору СУ ECP Veil, используется команда

 # net conf ports

3.3.5.5.6. Для проверки сопоставления имен интерфейсов с физическими портами на самом сервере используется команда

 # net conf ports blink

3.3.5.5.7. Изменение настроек IP-адреса для виртуального сетевого интерфейса управления «veil-mgmt» выполняется командой

 # net conf ip

3.3.5.5.8. Управление vlan-тегом для физических интерфейсов СУ ECP Veil выполняется командой

 # net conf vlan

3.3.5.5.9. Управление агрегацией для физических интерфейсов СУ ECP Veil выполняется командой

 # net conf bonds

3.3.5.5.10. Для интерфейса управления «veil-mgmt» используется команда

 # net conf ports set-default-bond

3.4. Первоначальная настройка ECP Veil

3.4.1. Вход в систему

3.4.1.1. Для первоначальной настройки ECP Veil необходимо авторизоваться в Web-интерфейсе управления кластером с пользователем, имеющим права администратора. СУ ECP Veil доступна по IP-адресу, полученному при установке автоматически либо заданному вручную для сервера, выполняющего роль контроллера.

3.4.1.2. При открытии интерфейса управления в браузере откроется окно авторизации, в котором необходимо ввести имя пользователя и пароль:

– имя пользователя – admin;

– пароль «по умолчанию» – veil.

– выбрать язык интерфейса.

3.4.2. Регистрация лицензионного ключа

3.4.2.1. Регистрация лицензионного ключа выполняется только через Web-интерфейс.

3.4.2.2. Для просмотра действующей лицензии используется раздел «Настройки» – «Лицензирование».

3.4.2.3. В данном разделе содержится информация по действующему лицензионному ключу ECP Veil, содержащая:

– лицензия на ПО;

– e-mail;

– компания;

– количество серверов;

– дней до окончания лицензии;

– дней до окончания сервисной поддержки;

– дата завершения лицензии;

– дата завершения сервисной поддержки.

3.4.2.4. Для установки лицензионного ключа активации необходимо выполнить следующие действия:

– вставить компакт-диск «Ключ активации»;

– нажать на кнопку «Выбрать файл лицензии»;

– в стандартном окне загрузки файлов выбрать файл формата «key», находящийся на компакт-диске, и нажать «Открыть»;

– далее обновить информацию по кнопке  .

3.4.3. Пользователи и роли

3.4.3.1. Управление параметрами собственной учетной записи производится в разделе «Настройки» – «Пользователи». Для просмотра информации о пользователе необходимо нажать на имя пользователя в списке.

3.4.3.2. Если пользователю назначена роль администратора безопасности или выше, то ему будет доступно управление учетными записями других пользователей в разделе «Настройки» – «Пользователи»:

– создание нового и деактивация (прекращение работы) имеющегося пользователя;

– изменение пароля другого пользователя.

Прекращение работы пользователя в системе осуществляется посредством изменения статуса учетной записи на «Неактивный». При этом все действия пользователя, произведенные им ранее и зафиксированные в системных журналах, сохранят связь с этим пользователем.

3.4.3.3. В системе предусмотрен ролевой метод разграничения доступа. Существуют следующие типы пользователей (пользовательские роли):

– «суперпользователь»;

– «администратор»;

– «администратор безопасности»;

– «администратор сети»;

– «администратор хранилищ»;

– «администратор ВМ»;

– «оператор ВМ»;

– «только чтение».

Для пользователя со встроенной учётной записью администратора «admin» применяется роль «суперпользователя». Для него доступны все настройки кластера.

При использовании встроенной базы данных пользователей роль «суперпользователя» может иметь только пользователь со встроенной учётной записью «admin».

При применении ролевой модели система управления кластером считает приоритетными запрещающие правила.

Для пользователя с ролью «администратор» действуют следующие ограничения:

– управление службами каталогов;

– управление SSL-сертификатами;

– управление лицензированием.

Для пользователя с ролью «администратор безопасности» действуют следующие ограничения:

– разрешено чтение всех параметров кластера;

– разрешено управление службами каталогов;

– разрешено управление SSL-сертификатами;

– разрешено управление пользователями.

Для пользователя с ролью «администратор сети» действуют следующие ограничения:

– разрешено чтение всех параметров кластера;

– разрешено управление сетевой подсистемой кластера;

– разрешено управление сетевыми интерфейсами ВМ.

Для пользователя с ролью «администратор хранилищ» действуют следующие ограничения:

– разрешено чтение всех параметров кластера;

– разрешено управление подсистемой хранения кластера;

– разрешено управление дисками ВМ и образами CD/DVD дисков.

Для пользователя с ролью «администратор ВМ» действуют следующие ограничения:

– разрешено чтение всех параметров кластера;

– разрешено управление ресурсами размещения ВМ;

– разрешено управление пулами данных;

– разрешено управление ВМ;

– разрешено управление доступом пользователей к ВМ.

Для пользователя с ролью «оператор ВМ» действуют следующие ограничения:

– разрешено чтение всех параметров кластера;

– управление ВМ, владельцем которых он является;

– предоставление доступа других пользователей к ВМ, владельцем которых он является.

Для пользователя с ролью «только чтение» действует ограничение – все объекты интерфейса управления доступны только для просмотра.

3.4.3.4. В системе реализована поддержка авторизации пользователей из Windows AD посредством LDAP. Настройка данных параметров доступна для ролей «суперпользователь» и «администратор безопасности».

Для регистрации внешних пользователей необходимо в разделе «Настройка» – «Службы каталогов»:

– добавить подключение к внешнему LDAP-серверу;

– для каждого LDAP-сервера настроить сопоставление пользователей (групп пользователей) с ролями системы управления кластером.

Если никакого сопоставления групп или пользователей AD не производилось, то все LDAP-пользователи могут зарегистрироваться в системе и иметь роль «оператор ВМ».

В отличии от встроенной базы данных пользователей для Windows AD допускается назначать пользователю или группе роль «суперпользователя».

3.4.3.5 В системе реализована поддержка технологии Single Sigh-On (SSO). Для её подключения необходимо:

– на контроллере Active Directory (AD) создать пользователя с соответствующими правами (администратора домена или разрешить набор прав для проверки пользователей через сетевой протокол безопасной идентификации/аутентификации Kerberos);

– зарегистрировать в Windows DNS доменное имя для контроллера(ов) ECP Veil;

– сформировать на контроллере домена Kerberos (keytabs) файл, по которому контроллер ECP Veil будет авторизовываться в AD.

Kerberos (keytabs) файл загружается для целевой службы каталогов на вкладке «Keytabs» интерфейса управления ECP Veil.

В окне, открывающемся по кнопке «Конфигурация SSO», вносятся данные, с которым будет проходить авторизация:

– параметры пользователя AD (имя пользователя и пароль);

– доменное имя контроллера ECP Veil.

В данном окне имя пользователя и DNS-имя контроллера ECP Veil вносится без указания имени домена AD.

Если в качестве основного DNS-сервера для ECP Veil не установлен DNS Windows AD, то поля «admin_server» и «kdc_urls» можно указывать в виде IP-адреса контроллера Windows AD.

3.4.4. Настройка глобальных параметров

3.4.4.1. Настройка сетевой подсистемы

3.4.4.1.1. Настройка сетевой подсистемы кластера производится в разделе «Сети» и описана в руководстве оператора ИСКП.00021-01 34 01.

3.4.4.2. Настройка отказоустойчивости

3.4.4.2.1. Основной частью отказоустойчивости является настойка высокой доступности (ВД) ВМ в составе кластера. Важным моментом защиты ВМ, предотвращающим восстановление ВМ на новом сервере до полного останова её копии на аварийном оборудовании, является управление сервером по IPMI. Поэтому, без получения от сервера сигнала об отключении питания, ВМ не будет перезапущена на новом сервере. Для серверов, не оборудованных IPMI, предусмотрена возможность признания сервера выключенным автоматически, что может привести к повреждению диска ВМ из-за попыток записи данных на один диск двумя экземплярами ОС ВМ.

3.4.4.2.2. Настройка высокой доступности, применяемая на весь кластер, настраивается в разделе «Кластеры». Для каждого кластера доступно применение индивидуальных настроек.

3.4.4.2.3. Количество попыток – это изменяемое число попыток запуска ВМ, по истечении которых система считает, что восстановление ВМ невозможно.

3.4.4.2.4. Интервал перезапуска – это пауза, в секундах, применяемая между попытками перезапуска ВМ.

3.4.4.2.5. Включение ВД для всего кластера будет означать, что для всех ВМ, параметры которых позволяют применить к ним ВД, будет активирована данная опция.

3.4.4.2.6. Автоматический выбор сервера – опция, позволяющая выбирать наименее загруженный сервер.

3.4.4.2.7. Таблица серверов, используемых для ВД, позволяет ограничивать список серверов, на которых будут восстанавливаться ВМ. Данная опция недоступна при автоматическом выборе целевого сервера для восстановления ВМ.

3.4.4.2.8. Необходимо учитывать, что индивидуальные настройки ВМ (при включенной ВД) перекрывают настройки кластера.

3.4.4.2.9. При использовании ограниченного списка серверов, участвующих в ВД, добавляемые в кластер серверы, попадают в список «Нераспределенные серверы».

3.4.4.2.10. Процедура добавления серверов в состав кластера подробно описана в разделе 3 руководства оператора ИСКП.00021-01 34 01.

3.4.4.3. Подключение, проверка работы и переключение на резервный контроллер

3.4.4.3.1. Для начала использования схемы с резервным контроллером необходимо выполнить следующие операции:

– установить ещё один экземпляр ПО ECP Veil в варианте «Controller + Node»;

– инициировать связанность экземпляров контроллера;

– назначить роли контроллеров;

– проверить репликацию данных.

3.4.4.3.2. Установка экземпляра контроллера производится в соответствии с 3.3.5.1 «Установка контроллера». Производить добавление данного экземпляра в кластер не обязательно. При необходимости добавить данный экземпляр в кластер перед началом работ следует добавить его как обычный сервер-node из UI-управления кластером. Использование в качестве самостоятельного контроллера перед добавлением не допускается.

После установки второго экземпляра, если контроллеры не находятся в одной подсети, необходимо обеспечить сетевую связанность до основного контроллера.

3.4.4.3.3. Инициация связи между экземплярами контроллера производится командой из CLI каждого экземпляра контроллера

 # system controller add <IP_второго_контроллера>

При выполнении данной команды необходимо указать пароль пользователя «root» второго контроллера.

В результате выполнения оба контроллера обменяются ключами SSH и будут готовы к репликации данных о настройках кластера с основного на резервный контроллер.

3.4.4.3.4. Назначение ролей контроллеров производится командами из CLI интерфейса:

 # system controller role slave

 # system controller role master

Первым необходимо инициировать резервный контроллер. В результате применения роли резервного контроллера будут выполнены операции:

– прекращение возможности входа на UI резервного контроллера;

– остановка системы очередей пользовательских и системных задач;

– сервер БД конфигурации кластера переведен в режим «slave».

После этого резервный контроллер попытается подключиться к «master» для получения данных о текущей конфигурации кластера.

Инициация основного контроллера как «master» – обязательная операция.

3.4.4.3.5. Проверка репликации производится командой

 # system controller status

3.4.4.3.6. Переключение ролей контроллера производится по схеме:

1) в случае штатного переключения:

– перевести master-контроллер в «slave» режим командой

 # system controller role slave

– перевести slave-контроллер в режим «master» командой

 # system controller role master

2) в случае аварии master-контроллера:

– при аварийном отключение master-контроллера выполнить на резервном контроллере команду в CLI

 # system controller role master

В результате будет восстановлена работа системы очередей постановки задач и возвращена возможность авторизации в Web-UI управления кластером;

– при восстановлении работы аварийного контроллера перевести его в режим «slave» для синхронизации изменений с контроллером, выполнявшим роль мастера.

Перевод восстановленного из аварии контроллера в «slave» – обязательная операция.

3.4.4.3.7. Для отключения режима с несколькими контроллерами необходимо выполнить следующие операции:

– сначала отключить репликацию данных на slave-контроллере, потом на master-контроллере командой в CLI

 # system controller role alone

– после этого на всех контроллерах удалить ключи SSH командой в CLI

 # system controller del

3.4.5. Настройка программы

3.4.5.1. Последовательность настройки программы и описание команд, используемых в процессе настройки и выполнения программы, приведены в руководстве оператора ИСКП.00021-01 34 01.

3.4.6. Обновление программы

3.4.6.1. Обновление программы осуществляется из CLI-интерфейса контроллера. При запуске команды обновления на контроллере также обновляются все серверы в составе кластера. В процессе обновления контроллер выступает в роли поставщика обновлений всем подключенным к кластеру серверам. Для обновления используется команда в CLI

 # upgrade

3.4.6.2. Перед обновлением можно сделать резервную копию конфигурации системы командой

 # backup

Восстановление из резервной копии также производится этой командой.

3.4.6.3. Для демонстрационной версии продукта обновления могут быть недоступны. Для получения обновленной версии необходимо обратиться к поставщику.

3.4.6.4. Доступ к командам CLI-интерфейса осуществляется после авторизации в консоли контроллера пользователя с учетной записью «root» и паролем, заданным при установке ОС.

3.4.7. Обслуживание программы

3.4.7.1. Для обслуживания программы в CLI-интерфейсе предусмотрен ряд команд:

– # *poweroff* – выключение сервера;

– # *reboot* – перезагрузка сервера;

– # *services {start* | *stop* | *restart* | *list}* – контроль состояния служебных сервисов;

– # *backup* – резервное копирование параметров системы.

4. ПРОВЕРКА ПРОГРАММЫ

4.1. Самотестирование программы

4.1.1. При включении серверной платформы автоматически запускается ECP Veil и начинается процедура самотестирования, при этом осуществляются проверки целостности файловой системы.

4.2. Результаты тестирования

4.2.1. Результаты тестирования выдаются на консоль сервера в процессе загрузки.

4.2.2. В консоли сервера, перед приглашением ввода имени пользователя, отображается IP-адрес, присвоенный интерфейсу управления сервером.

4.2.3. После авторизации в системе суперпользователя «root» предоставляется интерфейс CLI для управления параметрами сервера из консоли. Этот интерфейс предназначен для настройки параметров, влияющих на целостность кластера. Из данного интерфейса можно получить информацию о настройке сетевой подсистемы и произвести устранение неполадок.

5. СООБЩЕНИЯ СИСТЕМНОМУ ПРОГРАММИСТУ

5.1. Действия системного программиста должны осуществляться в соответствии с подсказками, выдаваемыми в процессе инсталляции и настройки программы на экране монитора.

5.2. Подсказка по командам CLI-интерфейса вызывается командой

 # help

ПРИЛОЖЕНИЕ

ПОЛНЫЙ ПЕРЕЧЕНЬ КОМАНД CLI ДЛЯ КОНСОЛЬНОГО УПРАВЛЕНИЯ ECP VEIL

1. Общая информация

1.1. Для стандартных команд Linux функциональность может быть ограничена. Это сделано для предотвращения внесения изменений в настройки системы, которые могут повлечь за собой нарушение ее работы.

1.2. Интерфейс управления «veil-mgmt» является виртуальным. Оперируя настройками данного интерфейса, надо учитывать, что взаимодействие данного интерфейса с физической сетью осуществляется через виртуальный коммутатор «veil-default» и подключенный в него физический(е) интерфейс(ы). Применяя настройки к «veil-mgmt», необходимо согласовать настройки сетевой подсистемы сервера и физических коммутаторов для беспрепятственного обмена трафиком между всеми серверами кластера.

1.3. Для всех команд, доступных через CLI (кроме стандартных команд Linux), используется ключ «–h» для получения подсказки по команде.

1.4. Для ряда команд настройки сетевой подсистемы доступен флаг «--check-conn». Он указывает, надо ли проверять связь с контроллером («по умолчанию» – нет).

2. Список стандартных команд Linux, доступных из CLI

2.1. Список стандартных команд Linux, доступных из CLI, приведен в таблице 1.

2.2. Для получения более подробной информации по командам (назначение ключей, опций, команд; порядок записи и выполнения) необходимо вывести справку по соответствующей команде, набрав после команд ключ «--help» и нажав клавишу «Enter». Например,

#date --help

2.3. Для получения информации о версии (для ряда команд) необходимо после ввода соответствующей команды набрать ключ «--version» и нажать клавишу «Enter». Например,

#date --version

Таблица 1

Команда	Описание
#help	Помощь по доступным в CLI командам
# <command> --help	Помощь по определенной команде. <command> – команда из таблицы 1. Например, «#date --help»
# <command> --version	Информация о версии. <command> – команда из таблицы 1. Например, «#date --version»
#df [[-a] [-B] [-H] [-h] [-l] [-k] [-l] [-P] [-T] [-t] [-x] [-v]] [file]	Использование места на дисках
#date [[-d] [-f] [-I [FMT]] [-r] [-R] [-s] [-u]] [+FORMAT]	Информация о текущей дате
#dmesg [-C] [-c] [-D] [-E] [-F <file>] [-f <list>] [-H] [-k] [-L [=<when>]] [-l <list>] [-n <level>] [-P] [-p] [-r] [-S] [-s <size>] [-u] [-w] [-x] [-d] [-e] [-T] [--notime | time-format <format>]	Просмотр событий
#free [-b] [-k] [-m] [-g] [-h] [-l] [-t] [-s <N>] [-c <N>] [-w]	Использование оперативной памяти
#ifconfig [-a] [-v] [-s] <interface> [[<AF>] <address>] [add <address> [/prefixlen]] [del <address> [/prefixlen]] [[-] broadcast [<address>] [[-] pointopoint [<address>] [netmask <address>] [dstaddr <address>] [tunell <address>] [outfull <NN>] [keepalive <NN>] [hw <HW> <address>] [mtu <NN>] [[-] trailers] [[-] arp] [[-] allmulti] [multicast] [[-] promisc]	Настройки сетевых интерфейсов

Команда	Описание
[mem_start <NN>] [io_addr <NN>] [irq <NN>] [media <type>] [txqueuelen] <NN> [[-] dynamic] [up | down]	
#iostat [-c] [-d] [-h] [-k] [-m] [-N] [-s] [-t] [-v] [-x] [-y] [-z] [-j {ID | LABEL | PATH | UUID}] [--dec={0 | 1 | 2} [--human] [-o JSON] [[-H] –g <group_name>] [-p [<device> [,…] | ALL]] [<device> […] | ALL]	Использование операций ввода-вывода
#ip [a] [ad] [add] [addr] [addre] [address] [route]	Настройки сетевой подсистемы (расширенные)
#ipmi-sensors [-D] [-h] [-u] [-p] [-P] [-k] [-K] [-a] [-I] [-l] [-W] [-B] [-C] [-F] [-E] [-v] [-i] [-q] [-r] [-R] [t] [T] [-L] [-b]	Сбор показаний датчиков аппаратной платформы
#ipmitool [lan] [print] [sdr] [sensor] [session] [sel]	Настройки BMC аппаратной платформы
#lsblk [[-a] [-b] [-d] [-D] [-z] [-e <list>] [-f] [-i] [-I <list>] [-J] [-l] [-T] [-m] [-n] [-o] [-O] [-p] [-P] [-r] [-s] [-S] [-t] [--sort <column> | --sysroot <dir>]] [<device> …]	Информация о подключенных блочных устройствах
#lscpu [-a] [-b] [-c] [-J] [-e [=<list>]] [-p [=<list>]] [-s <dir>] [-x] [-y]	Информация о процессорах системы
#lspci [-mm] [-t] [-v] [-k] [-x] [-xxx] [-xxxx] [-b] [-D] [-n] [-nn] [-q] [-qq] [-Q] [-s [[[[<domain>] :] <bus> :] [slot] [.[func]]] [-d [<vendor>] : [<device>] [: <class>]] [-i <file>] [-p <file>] [-M] [-A <metod>] [-O <par>=<val>] [-G] [-H <mode>] [-F <file>]	Информация о PCI-устройствах системы
#lsusb [-v] [-s] [-d] [-D] [-t] [-V]	Информация о подключенных USB-устройствах

Команда	Описание
#mount [-v] [-l]	Информация о примонтированных хранилищах
#mpstat [[-A] [-n] [-u] [-V] [-I {SUM | CPU | SCPU | ALL}] [-N {<node_list> | ALL}] [--dec={0 | 1 | 2}] [-o JSON] [-P {<cpu_list> | ALL}]] [<interval>] [<count>]	Информация о загрузке CPU
#multipath [-ll]	Информация о сетевых блочных устройствах (iSCSI, FC)
#netstat [-r] [-i] [-g] [-s] [-M] [-v] [-w] [-n] [-N] [-e] [-p] [-o] [-c] [-l] [-a] [-F] [-C] [-Z]	Информация о портах/сокетах
#numastat [-c] [-m] [-n] [-p <PID>] | <pattern>] [-s [<node>]] [-v] [-V] [-z] [<PID> | <pattern> …]	Информация окружения NUMA
#ping [-c <count>] [-i <interval>] [-I <interface>] [-m <mark>] [-M <mptudisc_option>] [[-l] preload] [-p <pattern>] [-Q <tos>] [-s <packetsize.] [-S <sndbuf>] [-t <tt>] [-T <timestamp_option>] [-w <deadline>] [-W <timeout>] [hop1 …] destination	Проверка сетевой связанности с другими узлами сети
#swapon [-s] [--show]	Информация об области на жестком диске, являющейся областью подкачки
#ps	Информация о запущенных процессах
#timedatectl [-h] [-H] [-M] [-p] [-a] [status] [show] [set-time <TIME>] [set-timezone <ZONE>] [list-timezones] [set-local-rtc <BOOL>] [set-ntp <BOOL>] [timesync-status] [show-timesync]	Информация о системном времени
#top [-d <secs>] [-n <max>] [-u <user>| U <user>] [-p <pid(s)>] [-o <field>] [-w] [cols]	Информация о запущенных процессах

Команда	Описание
#tzselect [-c <COORD>] [-n <LIMIT>]	Возможность выбора временной зоны
#uname [-a] [-s] [-n] [-r] [-v] [-m] [-p] [-i] [-o]	Информация о рабочей среде (типе операционной системы)
#virt-host-validate [-q] [[qemu] [lxc] [bhyve]]	Проверка аппаратной виртуализации и IOMMU включенного ядром
#zdb [[-b] [-c] [-C] [-d] [-D] [-E] [-h] [-i] [-l] [-k] [-L] [-m] [-M] [-O] [-R] [-s] [-S] [-v]] [[-A] [-e] [-F] [-G] [-I] [-o] [-p] [-P] [-q] [-t] [-u] [-U] [-V] [-x] [-X] [-Y]]	Информация о состоянии zfs
#zfs [list] [name] [available] [used] [type] [mounted] [mountpoint] [-H] [-o]	Информация о состоянии zfs
#zpool [list] [status] [name] [size] [free] [health] [events] [history] [-o] [-vH] [-v] [-x]	Информация о состоянии zfs

3. Последовательность действий при оффлайн-обновлении и описание состояний

3.1. Последовательность действий при оффлайн-обновлении и описание состояний приведены в таблице 2.

Таблица 2

Команды CLI ECP Veil	Команды CLI внешнего компьютера	Файлы на USB-накопителе	Состояние баз APT ECP Veil	Состояние кэша пакетов ECP Veil
upgrade local prepare --phase update	–	update.sig	old	old
перенос накопителя на внешний компьютер		update.sig	old	old
–	apt-offline get --bundle update.zip update.sig	update.zip, ~~update.sig~~	old	old

Команды CLI ECP Veil	Команды CLI внешнего компьютера	Файлы на USB-накопителе	Состояние баз APT ECP Veil	Состояние кэша пакетов ECP Veil
перенос накопителя на систему ECP Veil		update.zip, ~~update.sig~~	old	old
upgrade local proceed --phase update	–	update.zip, ~~update.sig~~	new	old
upgrade local prepare --phase upgrade	–	upgrade.sig, ~~update.zip,~~ ~~update.sig~~	new	old
перенос накопителя на внешний компьютер		upgrade.sig, ~~update.zip,~~ ~~update.sig~~	new	old
–	apt-offline get --bundle upgrade.zip upgrade.sig	upgrade.zip, ~~upgrade.sig,~~ ~~update.zip,~~ ~~update.sig~~	new	old
перенос накопителя на систему ECP Veil		upgrade.zip, ~~upgrade.sig,~~ ~~update.zip,~~ ~~update.sig~~	new	old
upgrade local proceed --phase upgrade	–	upgrade.zip, ~~upgrade.sig,~~ ~~update.zip,~~ ~~update.sig~~	new	new
upgrade start	–	~~upgrade.zip,~~ ~~upgrade.sig,~~ ~~update.zip,~~ ~~update.sig~~	ПО системы обновлено	
Примечание. Перечёркнутое имя говорит о необязательности файла для работы.				

Перечень принятых сокращений

ВД	– высокая доступность
ВМ	– виртуальная машина
МК	– менеджер конфигурации
НЖМД	– накопитель на жёстком магнитном диске
ОС	– операционная система
ПО	– программное обеспечение
ПЭВМ	– персональная электронно-вычислительная машина
СУ	– сеть управления
ТОС	– технологическая операционная система
ЦСХД	– централизованная система хранения данных
ЭВМ	– электронно-вычислительная машина
AD	– Active Directory (активный каталог)
ECP	– Enterprise Cloud Platform (облачная платформа корпоративного уровня)
PXE	– Preboot Execution Environment (среда для загрузки компьютера с помощью сетевой карты без использования локальных носителей данных)
SSO	– Single Sigh-On (технология единого входа)

Для заметок

масштаб
научно-
исследовательский
институт

194100, Санкт-Петербург, ул. Кантемировская д.5, лит. А,
(812) 309-03-21, sales@mashtab.org
www.mashtab.org