УТВЕРЖДЕН

РАМГ.46653-03 32 01-ЛУ

Подп. и дата	
Инв. № дубл.	
Взам. инв. №	
Подп. и дата	
Инв. № подл.	

СПО «ВИРТУАЛЬНОЕ ПРОСТРАНСТВО»

Руководство системного программиста

РАМГ.46653-03 32 01

Листов 84

2022

Литера

АННОТАЦИЯ

Данный документ является руководством системного программиста СПО «Виртуальное пространство» (далее по тексту – СПО ВП) для аппаратной платформы (АП) на базе процессоров «Эльбрус-16С» и операционной системы (ОС) «Альт Сервер для Эльбрус».

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

Настоящее руководство входит в состав эксплуатационной документации и рассчитано на системного программиста, имеющего навыки работы и администрирования ОС семейства Linux.

СОДЕРЖАНИЕ

Лист

1. ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

1.1. Назначение программы

1.1.1. СПО ВП предназначено для работы в составе комплекта для построения комплексной системы обеспечения и управления безопасностью.

1.1.2. СПО ВП обеспечивает создание и администрирование виртуальной инфраструктуры для аппаратных платформ на базе процессоров «Эльбрус-16С» с аппаратной поддержкой виртуализации.

1.1.3. СПО ВП обеспечивает создание и управление виртуальной инфраструктурой как на отдельной серверной платформе, так и на кластерной системе (группе серверных платформ).

1.1.4. СПО ВП обеспечивает возможность автоматической настройки нового физического сервера в момент добавления его в кластер.

1.1.5. СПО ВП обеспечивает создание следующих типов объектов и управление ими:

– физический сервер;

– виртуальная машина (ВМ);

– виртуальная сеть;

– пул хранения данных;

– виртуальный диск;

– образ оптического диска;

– шаблон виртуальной машины.

1.1.6. СПО ВП поддерживает запуск гостевых операционных систем (ОС):

– для архитектуры Эльбрус;

– для архитектуры x86_64.

Примечание. Гостевые ОС для архитектуры x86_64 запускаются в режиме двоичной трансляции. Данная возможность должна поддерживаться гостевой ОС.

1.1.7. СПО ВП обеспечивает возможность инсталляции ОС внутри ВМ с образа оптического диска в формате ISO 9660 и UDF.

1.1.8. СПО ВП обеспечивает создание, хранение и импорт шаблонов ВМ для автоматического развертывания виртуальных машин.

1.1.9. СПО ВП обеспечивает создание шаблона ВМ из виртуальной машины, инсталлированной с образа оптического диска.

1.1.10. СПО ВП обеспечивает для платформ, имеющих аппаратную поддержку виртуализации, возможность монополизации виртуальными машинами физических компонентов аппаратной платформы, подключенных к интерфейсам SATA, PCI, PCI-E, USB, Serial.

1.1.11. СПО ВП обеспечивает использование в качестве пулов хранения данных:

– необщие хранилища;

– общие хранилища.

1.1.12. СПО ВП обеспечивает использование локальных групп томов LVM (VG LVM) на вычислительных узлах в качестве локальных хранилищ данных.

1.1.13. СПО ВП обеспечивает использование внешних систем хранения данных, подключаемых по протоколу NFS, в качестве общих хранилищ.

1.1.14. СПО ВП обеспечивает использование распределенных хранилищ данных в качестве общих хранилищ.

1.1.15. СПО ВП обеспечивает возможность переноса ВМ между физическими серверами, объединенными в кластер, находящимся под управлением одного экземпляра СПО ВП.

1.1.16. СПО ВП обеспечивает поддержку переноса виртуальных дисков между пулами хранения данных.

1.1.17. СПО ВП при помощи средств интерфейса управления обеспечивает выполнение следующих операций над ВМ:

– создание ВМ из шаблона;

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

– редактирование параметров ВМ;

– создание шаблона ВМ;

– запуск;

– остановка;

– перезагрузка;

– клонирование ВМ;

– создание копии состояния ВМ (снэпшот ВМ);

– восстановление состояния текущей ВМ из копии;

– создание новой ВМ из копии состояния.

1.1.18. В СПО ВП при создании ВМ обеспечивает возможность задания следующих параметров:

– имя ВМ;

– описание ВМ;

– количество виртуальных процессоров;

– количество оперативной памяти;

– количество дискового пространства;

– количество сетевых интерфейсов и их сопоставление с виртуальными сетями;

– имя шаблона (при создании из шаблона);

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

– выбор существующего или создание нового виртуального диска;

– пул для хранения виртуального диска.

1.1.19. СПО ВП имеет возможность опционально задавать количество виртуальных процессоров при создании ВМ.

1.1.20. СПО ВП при помощи средств интерфейса управления обеспечивает выполнение следующих операций над виртуальными дисками:

– создание;

– уничтожение;

– клонирование;

– перенос виртуального диска в другой пул хранения данных;

– подключение (отключение) диска от ВМ.

1.1.21. При создании виртуального диска в СПО ВП обеспечивается возможность задать следующие параметры:

– имя виртуального диска;

– пул хранения для размещения виртуального диска;

– количество дисковой памяти.

1.1.22. СПО ВП обеспечивает возможность работы виртуальных машин в режиме высокой доступности.

1.1.23. СПО ВП обеспечивает работу ВМ в режиме высокой доступности путем автоматического перезапуска на резервном вычислительном узле ВМ, которые были запущены на отказавшем вычислительном узле.

Примечания:

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

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

1.1.24. СПО ВП обеспечивает время запуска процедуры восстановления работы ВМ, запущенной в режиме высокой доступности, не более 5 минут.

1.1.25. СПО ВП обеспечивает создание изолированных виртуальных сетей между ВМ.

1.1.26. СПО ВП для управления использует Web-ориентированный графический интерфейс и REST-API.

1.1.27. СПО ВП обеспечивает возможность шифрования канала управления средствами протокола HTTPS.

1.1.28. СПО ВП обеспечивает вывод в интерфейс управления информации о текущем состоянии каждого физического сервера в кластере. Информация содержит:

– имя хоста;

– описание хоста;

– текущее состояние (доступен, недоступен);

– время последнего изменения состояния;

– количество запущенных виртуальных машин;

– процент загрузки процессора;

– количество свободной оперативной памяти;

– загрузка дисковой подсистемы ВМ;

– состояние локально подключенных дисков и количество свободного места на них;

– загрузка сетевых интерфейсов.

1.1.29. СПО ВП обеспечивает вывод в интерфейс управления следующей информации о каждой ВМ:

– имя ВМ;

– описание ВМ;

– текущее состояние;

– время последнего изменения состояния;

– время с момента включения;

– время создания ВМ;

– время последнего запуска (остановки) ВМ;

– пользователь, создавший ВМ;

– процент загрузки CPU ВМ;

– загрузка сетевых интерфейсов ВМ;

– загрузка дисковой подсистемы ВМ.

1.1.30. СПО ВП обеспечивает создание нескольких типов учетных записей с различным уровнем привилегий.

1.1.31. СПО ВП обеспечивает занесение в журнал записей о следующих событиях:

– авторизация пользователя в интерфейсе управления;

– ошибка аутентификации пользователя;

– запуск контроллера;

– изменение состояния физического сервера;

– добавление нового физического сервера;

– удаление физического сервера;

– время создания ВМ;

– запуск ВМ;

– остановка ВМ;

– уничтожение ВМ;

– миграция ВМ;

– создание копии состояния ВМ;

– клонирование ВМ.

1.2. Требования к техническим средствам

1.2.1. Для нормального функционирования СПО ВП требуется:

– не менее одного процессора с архитектурой Эльбрус-16С;

– оперативная память – не менее 20 Гбайт;

– жесткий диск объемом – не менее 100 Гбайт;

– устройство отображения графической информации (монитор);

– клавиатура;

– графический манипулятор типа «мышь»;

– устройство чтения/записи компакт-дисков в формате CD/DVD;

– устройство бесперебойного питания (опционально).

1.2.2. СПО ВП предназначен для использования на аппаратных платформах с архитектурой Эльбрус-16С.

1.2.3. Аппаратные требования к физическому серверу:

– материнская (процессорная) плата и процессор должны поддерживать технологию аппаратной виртуализации;

– каждый процессор должен иметь не менее четырех вычислительных потоков;

– объем установленной оперативной памяти должен быть не менее 20 Гбайт;

– каждый сервер должен иметь возможность установки не менее одного накопителя на жестком магнитном диске (НЖМД) с интерфейсом SATA/SAS;

– объем каждого установленного НЖМД должен быть не менее 100 Гбайт;

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

– каждый сервер должен иметь интерфейс управления IPMI (при наличии возможности аппаратной платформы);

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

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

1.2.4. Для установки СПО ВП 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, а также возможность выбора в BIOS сервера загрузки с диска;

– для установки с USB-накопителя должен быть USB-порт, а также возможность выбора в BIOS сервера загрузки с USB;

– для установки по сети должен быть сетевой интерфейс с поддержкой загрузки по протоколу PXE (Preboot Execution Environment), а также возможность выбора в BIOS сервера загрузки по сети;

– для установки через IPMI-интерфейс (при наличии возможности аппаратной платформы) в IPMI-интерфейсе должна быть поддержка подключения ISO-образа для загрузки.

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 СПО ВП в составе одного или двух физических серверов с (без) сети хранения данных с применением ограниченного функционала управления.

Примечание. Ограниченный функционал управления заключается в переводе в ручной режим управляющих механизмов миграции ВМ, отказоустойчивости и распределения ВМ по серверам.

1.2.6. Для корректной и полноценной работы СПО ВП необходимо:

– не менее одного выделенного интерфейса IPMI (при наличии возможности аппаратной платформы);

– 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 СПО ВП, необходимо учитывать, что для одной ВМ может быть выделено виртуальной памяти не более, чем установленной физической памяти.

1.2.9. Для работы в Web-интерфейсе необходимо наличие персональной электронно-вычислительной машины (клиента) и браузера со следующими характеристиками:

– браузер поддерживает протоколы HTTP/HTTPS;

– браузер поддерживает исполнение HTML5, TypeScript и JavaScript кода;

– браузер позволяет интерфейсу управления открывать дополнительные окна (вкладки).

Примечание. Необходимо обеспечить связь между сервером СПО ВП и клиентом (например, при помощи Ethernet-соединения, локальной сети, сети Интернет).

1.3. Совместимое оборудование

Далее приведен список оборудования, на котором успешно прошло тестирование СПО ВП на полную совместимость.

1.3.1. Сетевые коммутаторы

1.3.1.1. В таблице 1 приведен список совместимых сетевых коммутаторов.

Таблица 1

Производитель	Модель	Примечание
Cisco	SG550XG-8F8T	
Netgear	XS716T-100NES	
D-Link	DXS-1100-10TS	
D-Link	DXS-1200-12SC	
D-Link	DGS-1100-18	
Булат	BS2500-48G4S	
Huawei	S6270	
Русьтелетех	RTT-A311-24T-4XG	
Supermicro	SBM-GEM-X3S+	Для установки в шасси SBE-720
Supermicro	SBM-XEM-X10SM	Для установки в шасси SBE-720
Supermicro	MBM-XEM-002	Для установки в шасси MBE-314
Cisco	Nexus 4500 S Series	

1.3.2. Совместимые гостевые ОС

1.3.2.1. В таблице 2 приведен список совместимых гостевых ОС.

Таблица 2

Производитель	Модель	Конфигурация
МЦСТ	ОС Эльбрус (OSL)	–
ALT Linux Team	ALT Linux	–

1.4. Требования к программному обеспечению

1.4.1. В состав СПО ВП входят все компоненты, которые необходимы для его корректного функционирования. При соблюдении требования установки (обновления) программного обеспечения (ПО) только с дисков разработчика гарантируется корректное функционирование СПО ВП.

1.4.2. При необходимости использования дополнительного или стороннего ПО необходимо связаться со службой технической поддержки предприятия-разработчика.

1.5. Требования к квалификации специалистов

1.5.1. Специалист, производящий установку СПО ВП, должен иметь высшее инженерное образование и обладать знаниями, соответствующими специализации «Администратор Linux», «Администратор сетей передачи данных» в областях:

– установка и 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, LACP, VLAN на коммутаторах.

2. СТРУКТУРА ПРОГРАММЫ

2.1. Структура ПО

2.1.1. В программе реализован принцип модульного построения ПО, когда каждый отдельный модуль отвечает за решение узкоспециализированной задачи. Все ПО разделяется на несколько подсистем. Каждая подсистема в свою очередь разделяется на набор модулей, которые реализуют определенную специализированную задачу.

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

2.1.3. Структурная схема СПО ВП приведена на рис. 1.

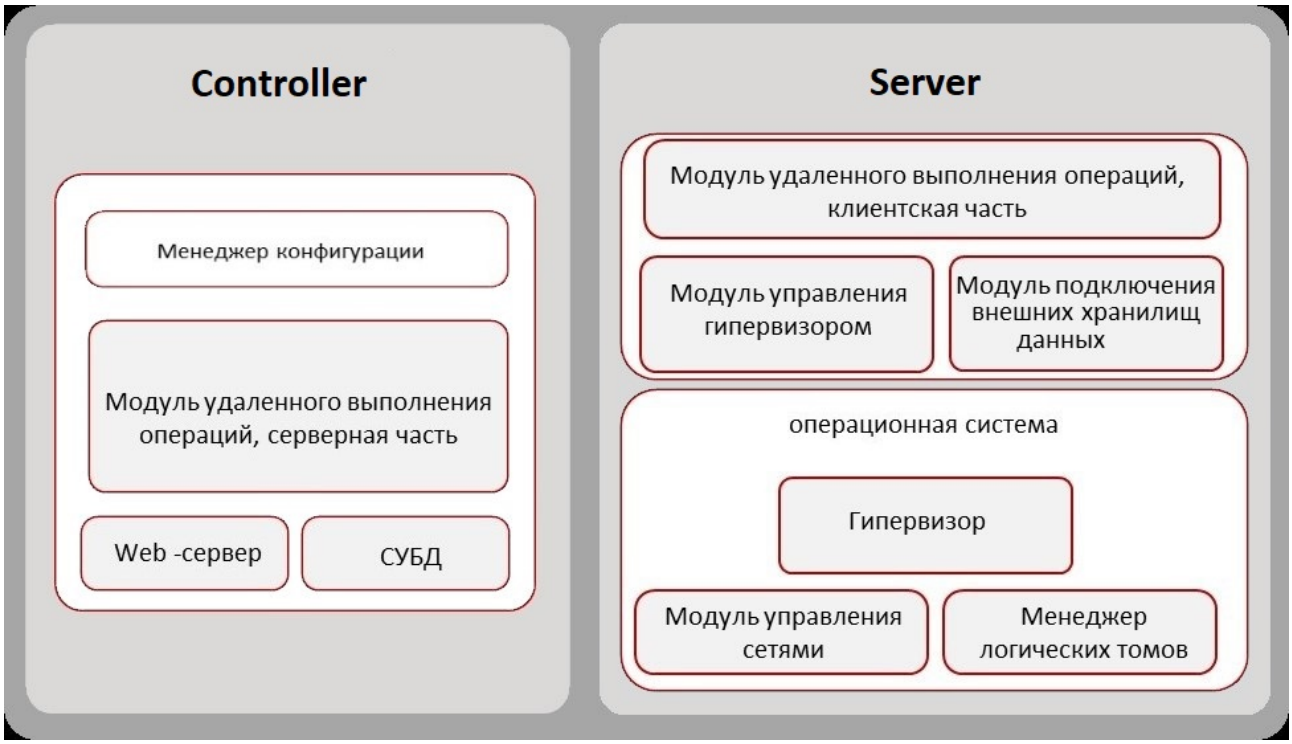

Рис. 1

2.1.4. Менеджер конфигурации (МК) представляет собой программный комплекс, предназначенный для управления СПО ВП.

В состав МК входят следующие используемые программные продукты:

– ПО, распространяемое в рамках лицензий GNU/GPL;

– ПО, распространяемое в рамках лицензий Apache License 2.0.

Web-интерфейс МК, RESTfull API-интерфейс и логика управления являются продуктами собственной разработки с применением языков программирования JavaScript, Python, bash, C, Ruby.

2.1.5. СПО ВП – это специальное программное обеспечение на базе ядра Linux, в состав которого входит комплект совместимых (проверенных) версий ПО, необходимый для его корректного функционирования. Обновление ПО в составе СПО ВП может проводиться только с дисков разработчика. Обновления из других источников не допускаются, иначе исполнитель (разработчик) не несет ответственности за ущерб, нанесенный данным клиента.

Примечание. При соблюдении требования установки (обновления) ПО только с дисков разработчика гарантируется корректное функционирование СПО ВП. При необходимости использования дополнительного или стороннего ПО необходимо связаться с технической поддержкой предпрятия-разработчика.

2.2. Управление ВМ

2.2.1. Запуск ВМ обеспечивается модулем-гипервизором «qemu-kvm», входящим в состав СПО ВП. Гипервизор «qemu-kvm» устанавливается во время установки СПО ВП.

2.3. Супервизор узла

2.3.1. Супервизор узла – это python-сервис в СПО ВП под именем в Command Line Interface (CLI) «node-engine». Сервис занимается запуском, остановом и мониторингом состояния дочерних демонов.

2.3.2. Список дочерних демонов указан в таблице 3 в порядке очередности запуска (может незначительно меняться в зависимости от версии).

Таблица 3

Название	Описание
RpcServer	Сервис связи с контроллером
RpcExecuteDaemon	Сервис выполнения операций от контроллера
DomainStatus	Сервис обработки статистики по ВМ (цикл раз в 5 секунд)
EventCollector	Сервис сбора сообщений о жизненном цикле от виртуальных машин

Название	Описание
DomainStatistics	Сервис отправки статусов виртуальных машин контроллеру (цикл раз в 5 секунд)
Ballooning	Сервис balloning узла (цикл раз в 5 секунд)
StorageStatus	Сервис распознавания всех подключенных хранилищ и их вложенных сущностей (цикл раз в 30 секунд)
HeartBeat	Сервис обновления состояния связи узла с контроллером и кворумом (цикл раз в 15 секунд)
StorageHeartbeat	Сервис связности узла с контроллером и кворумом через файлы в сетевых пулах данных (цикл раз в 5 секунд)
NetworkStatus	Сервис распознавания всех сетевых сущностей на узле (цикл раз в 30 секунд)
ClusterStatus	Сервис определения и работы лидера кластера (цикл раз в 30 секунд)
HardwareStatus	Сервис проверки состояния физического оборудования (цикл раз в 180 секунд)
LibvirtCollector	Сервис сбора детальной статистики виртуальных машин (цикл раз в 5 секунд)
ControllerEventListener	Сервис получения дополнительных сообщений от контроллера
SnmpMibExtender	Сервис сбора статистики и расширения стандартного MIB для получения специфичной информации (цикл раз в 30 секунд)
WsDataHandler	Сервис получения сигналов базы данных, фильтрования и отправления их демону терминации WS-соединений

2.4. Супервизор контроллера

2.4.1. Супервизор контроллера – это python-сервис в СПО ВП под именем в CLI «controller-engine». Сервис занимается запуском, остановом и мониторингом состояния дочерних демонов.

2.4.2. Список дочерних демонов указан в таблице 4 в порядке очередности запуска (может незначительно меняться в зависимости от версии).

Таблица 4

Название	Описание
GRPCManager	Демон связи с узлами
StorageEventListener	Демон, прослушивающий очередь со статусами хранилищ от узлов
NetworkEventListener	Демон, прослушивающий очередь со статусами сети от узлов
DomainEventListener	Демон, прослушивающий очередь со статусами ВМ от узлов
Events	Демон, сохраняющий сообщения о выполненных командах в CLI, сообщениях от узла и от загрузчика файлов
HeartBeatDaemon	Демон, осуществляющий проверку доступности узлов и ставящий задачи на ограждение недоступных узлов (цикл раз в 5 секунд)
NodeControllerManager	Демон управления узлами и контроллером
TaskProcessor	Демон выставления статусов и выполнения success/failed методов функций
TaskPreProcessor	Демон сбора результатов выполнения задач с узлов
MultiTaskProcessor	Демон обработки запросов на выполнение следующей по счету задачи в рамках мультизадач
MultiTaskLevelProcessor	Демон, реализующий логику запуска задач текущего уровня мультизадачи

Название	Описание
TaskChecker	Демон запуска задач по расписанию и проверки активных и завершенных задач на узлах (цикл раз в 15 секунд)
TaskProgressWatcher	Демон выставления прогресса задач после получения прогресса от узлов
DomainStatus	Демон обработки статистики ВМ с узлов
StorageStatus	Демон обработки статусов хранилищ с узлов
NetworkStatus	Демон обработки статусов сети с узлов
ClusterStatus	Демон проверки загрузки узлов и доступности ВМ (цикл раз в 90 секунд)
DRSDaemon	Демон распределения нагрузки между узлами (цикл раз в 5 секунд)
Fencer	Демон, осуществляющий ограждение узлов
RecoveryDaemon	Демон, поднимающий ВМ, которые помечены как «high available»
WsDataHandler	Сервис получения сигналов базы данных, фильтрования и отправления их демону терминации WS-соединений
ControllerHerald	Демон, получающий дополнительную информацию от API и рассылающий ее узлам

2.5. Описание сервисов

2.5.1. В таблице 5 приведен список сервисов (рис. 2) и их описание.

Таблица 5

Название	Описание	Расположение или просмотр журналов
controller-engine	Супервизор контроллера	/var/log/veil/controller/controller.log
controller-db (postgresql)	Postgresql (реляционная база данных супервизора контроллера, работа ведется через PgBouncer)	/var/log/postgresql

Название	Описание	Расположение или просмотр журналов
controller-web-api	Web-сервер контроллера	/var/log/veil/controller/django.log
controller-web-proxy	Асинхронный прокси-сервер контроллера между nginx и Web-сервером контроллера	/var/log/veil/controller/veil_async.log
controller-web-uploader	Асинхронный сервис контроллера загрузки файлов в пулы данных	/var/log/veil/controller/veil_async.log
controller-log-sender	Асинхронный сервис контроллера отправки логов внешней системе	/var/log/veil/controller/veil_async.log
controller-logger	Elasticsearch (движок и база данных журналов)	/var/log/elasticsearch-log/veil
controller-websocket	Асинхронный сервис WS-соединений (принимает запросы на подписки пользователей и отправляет данные об изменениях в базе данных подписчикам)	/var/log/veil/controller/veil_async.log
controller-statistics	Prometheus (база данных статистики)	/var/log/prometheus
node-engine	Супервизор узла	/var/log/veil/node/node.log
node-web-api	Web-сервер узла	/var/log/veil/node/django.log
node-web-proxy	Асинхронный прокси-сервер узла между nginx и Web-сервером контроллера	/var/log/veil/node/veil_async.log
node-web-uploader	Асинхронный сервис узла загрузки файлов в пулы данных	/var/log/veil/node/veil_async.log
node-statistics	prometheus-node-exporter (сервис сбора статистики о системе)	/var/log/syslog
td-agent	Fluentd based data collector for Treasure Data (сервис сбора журналов системы)	/var/log/td-agent
iscsi	iSCSI initiator сервис	/var/log/syslog

Название	Описание	Расположение или просмотр журналов
multipath	Device-Mapper Multipath Device Controller	/var/log/syslog
nginx	Граничный Web-сервер	/var/log/nginx
ntp	Сервис синхронизации времени	/var/log/syslog
redis	База данных супервизоров контроллеров и узлов NoSQL	/var/log/redis
beanstalkd	Сервис очередей	/var/log/syslog
snmp	Сервис SNMP	/var/log/syslog
gluster	Сервис кластерного транспорта типа «gluster»	/var/log/glusterfs
corosync	Сервис кворума кластерного транспорта типа «gfs2»	/var/log/corosync/corosync.log
dlm	Сервис блокировок и ограждения кластерного транспорта типа «gfs2»	dmesg
watchdog	Сервис слежения за «здоровьем» системы	/var/log/watchdog
consul	Сервис выбора лидера и базы данных кластера	/var/log/syslog

Примечание. Список сервисов отличается в зависимости от типа установки.

```
cli # services list
SERVICE NAME                              STATUS
controller-engine                         running
controller-db                             running
controller-web-api                        running
controller-web-proxy                      running
controller-web-uploader                   running
controller-log-sender                     running
controller-logger                         stopped
controller-websocket                      running
controller-statistics                     running
node-engine                               running
node-statistics                           running
node-logger                               running
iscsid                                    running
multipathd                                running
nginx                                     running
ntp                                       running
redis                                     running
snmp                                      stopped
gluster                                   running
corosync                                  running
dlm                                       running
watchdog                                  running
consul                                    stopped
```

Рис. 2

2.6. Схема системных пользователей

2.6.1. На рис. 3 приведена схема пользователей.

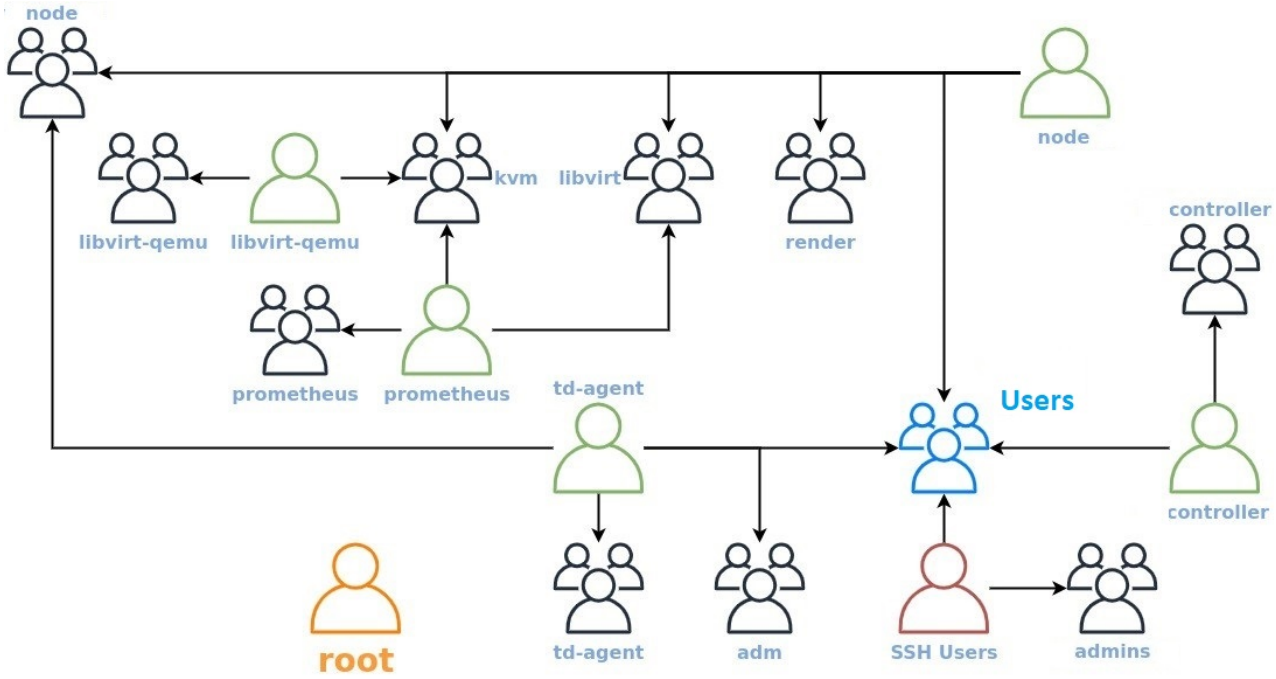

Рис. 3

«Users» – это общая группа системных пользователей.

«admins» – это группа SSH-пользователей.

Примечание. Схемы системных пользователей контроллера и узла идентичны.

2.7. Временные параметры системы

2.7.1. В таблице 6 приведены временные параметры системы, по достижению которых происходит проверка и изменение состояния.

Таблица 6

Название	Инициатор	Параметр	Описание
Автотестирование системы	cron, CLI, WEB	Ежесуточно (в 1 час 1 минуту ночи) и при запуске (инициализации) узла	Происходит проверка файлов конфигураций и контроль статусов сервисов
Сканирование ВМ	Супервизор узла (DomainStatus, LibvirtCollector)	5 секунд	Проверка статусов питания ВМ, связи с агентом, статистики
Сканирование хранилищ	Супервизор узла (StorageStatus)	30 секунд	Сбор всех сущностей хранилищ с размерами
Сканирование сетевых сущностей	Супервизор узла (NetworkStatus)	30 секунд	Сбор всех сущностей сети
Ballooning	Супервизор узла (Ballooning)	5 секунд	Контроль памяти ВМ
HardwareStatus	Супервизор узла (HardwareStatus)	180 секунд	Проверка состояния физического оборудования
Multitask divisor	Супервизор контроллера (MultitaskProcessor)	4	Количество параллельных задач в последовательных блоках мультизадач

3. УСТАНОВКА И БАЗОВАЯ НАСТРОЙКА

Установка и настройка программы осуществляется на сервер в следующей последовательности:

1) установка и настройка ОС «Альт Сервер 10.1 для Эльбрус» (см. 3.1);

2) установка и настройка программы СПО ВП (см. 3.3).

3.1. Установка и настройка ОС «Альт Сервер 10.1 для Эльбрус»

3.1.1. Для установки ОС «Альт Сервер 10.1 для Эльбрус» на аппаратную платформу необходимо загрузить ISO-образ ОС. Получить ISO-образ ОС «Альт Сервер 10.1 для Эльбрус» можно по запросу у предпрятия-разработчика ОС, его официального представителя или вендора. Порядок установки приведен в приложении 1 данного руководства.

3.1.2. После завершения установки ОС «Альт Сервер 10.1 для Эльбрус» необходимо войти в учетную запись «altlinux»

3.1.3. Перейти в режим суперпользователя «root», выполнив команду *su -* и введя пароль «bazalt».

3.1.4. Подключить репозитории «ALT Linux» с пакетами и обновлениями командами:

cat << EOF > /etc/apt/sources.list.d/pvt.list

rpm http://elbrus.ivk.ru/pvt/e2k/235a5dd6e4218b555c3cc4d5d854b0450780ef00/ repo/ e2kv6 classic

rpm http://elbrus.ivk.ru/pvt/e2k/235a5dd6e4218b555c3cc4d5d854b0450780ef00/ repo/ noarch classic

rpm http://elbrus.ivk.ru/pvt/e2k/237ce19817d5009c0c16ac80e3d3e94bc753280f/repo e2kv6 classic

rpm http://elbrus.ivk.ru/pvt/e2k/237ce19817d5009c0c16ac80e3d3e94bc753280f/repo noarch classic

EOF

3.1.5. Обновить и установить ядро с поддержкой виртуализации командой

apt-get update && apt-get install apt-get install kernel-image-mcst-e16c#5.4.193-alt5.9.4@1665000975

3.2. Проверка целостности СПО ВП

3.2.1. Непосредственно перед установкой должна быть проверена контрольная сумма установочного компакт-диска РАМГ.46653-03. Проверка контрольной суммы осуществляется на автоматизированном рабочем месте (АРМ) с установленной ОС «Astra Linux Special Edition» версия 1.6 в следующей последовательности:

– включить АРМ с установленной ОС и дождаться запроса входного имени;

– авторизоваться в системе под именем и паролем, который был указан при создании учетной записи;

– дождаться приглашения ввода консоли;

– получить привилегии «root», выполнив команду

sudo su

– вставить компакт-диск в технологический дисковод CD/DVD-ROM;

– смонтировать компакт-диск с помощью команды

mount /media/cdrom

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

cd /media/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

– дождаться окончания выполнения введенной команды (выключения индикатора активности дисковода);

– сравнить значение контрольной суммы, выведенное на экран, со значением контрольной суммы, приведенной на компакт-диске;

– размонтировать компакт-диск с помощью команд

cd /; umount /media/cdrom

– извлечь компакт-диск из технологического дисковода CD/DVD-ROM.

3.2.2. Программа считается готовой к установке, если контрольная сумма, отображенная на мониторе ЭВМ для компакт-диска РАМГ.46653-03, совпала с контрольной суммой этого диска, записанной в формуляре РАМГ.46653-03 30 01.

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

3.3. Установка и настройка СПО ВП

3.3.1. Установка СПО ВП выполняется на сервер с предварительно установленной ОС «Альт Сервер 10.1 для Эльбрус».

3.3.2. Войти в ОС с учетной записью пользователя «altlinux» и паролем «bazalt».

3.3.3. Перейти в режим суперпользователя «root», выполнив команду *su -* и введя пароль «bazalt».

3.3.4. Создать директорию для размещения дистрибутива и дополнительных пакетов командой

mkdir -p /var/repo/

3.3.5. Вставить в устройство чтения CD/DVD компакт-диск СПО ВП РАМГ.46653-03, смонтировать и скопировать содержимое диска в каталог «var/repo/ksoub» с помощью команд:

mount /dev/cdrom /mnt

cp -r /mnt /var/repo/ksoub

Подключить загруженный репозиторий командой

echo "rpm file:/var/repo/ksoub/build e2kv6 build" >> /etc/apt/sources.list.d/ksoub.list

Размонтировать компакт-диск командой

umount /mnt

Извлечь компакт-диск СПО ВП РАМГ.46653-03.

3.3.6. Вставить в устройство чтения CD/DVD диск с дополнительными пакетами «Технологический диск для установки СПО ВП».

Смонтировать и скопировать содержимое диска «Технологический диск для установки СПО ВП» в каталог «var/repo/extra» командой

mount /dev/cdrom /mnt

cp -r /mnt /var/repo/extra

Подключить загруженный репозиторий командой

echo "rpm file:/var/repo/extra/build e2kv6 build" >> /etc/apt/sources.list.d/extra.list

Размонтировать компакт-диск командой

umount /mnt

Извлечь «Технологический диск для установки СПО ВП».

3.3.7. Перейти в директорию с помощью команды

cd /var/repo/ksoub/installer

3.3.8. Сделать файл установщика исполняемым с помощью команды

chmod +x ./install.sh

3.3.9. Запустить установку с помощью команды

./install.sh

3.3.10. Далее в программе установки будет предложен вариант установки: «controller», «node» или «controller+node». Для установки в требуемой конфигурации необходимо выбрать соответствующую цифру и нажать «Enter» (рис. 3).

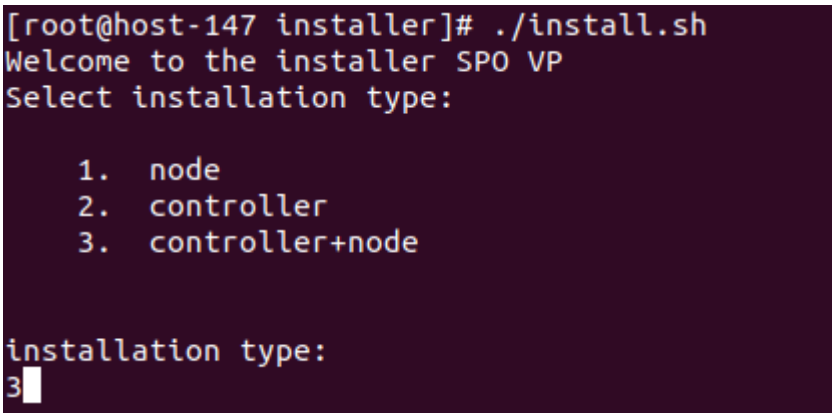

Рис. 4

В данном случае будет выбрана установка, соответствующая «controller+node».

3.3.11. Происходит процесс установки. После завершения установки сервер выдаст следующее сообщение «Press enter for reboot!».

В случае, если после нажатия «Enter» не произойдет перезагрузка сервера, необходимо его перезагрузить вручную.

3.3.12. После перезагрузки будет длительный процесс конфигурации сервера.

Примечание. В какой-то момент на сервере отключится сеть. Для уточнения, когда завершится процесс настройки, можно использовать команду *log*. Будет написано «Installation process is not yet completed, please wait. Type command 'log first_boot' for details». После завершения настройки надпись пропадет.

3.3.13. Для настройки сетевого соединения необходимо выбрать основной интерфейс с помощью команды

net conf ports set-default-port -i <имя интерфейса>

3.3.14. Посмотреть интерфейсы можно командой

net show ports

3.3.15. Указать сетевые настройки можно командой

net conf ip set-static -i <ip-address> -m <netmask> -g <gateway address>

3.3.16. Указать сервер имен можно командой

net conf dns set-static -n <dns ip addr>

3.3.17. Процесс установки завершен.

4. ОБНОВЛЕНИЕ ПРОГРАММЫ

4.1. Общие сведения об обновлении СПО ВП

Запуск установки обновлений необходимо выполнять на всех узлах по очереди.

ВНИМАНИЕ! Рекомендуется перед обновлениями перевести все узлы в «Сервисный режим».

ВНИМАНИЕ! Если во время обновления СПО ВП один или несколько узлов СПО ВП невозможно обновить, то необходимо выполнить обновление данных узлов в кратчайшее время до соответствующей версии.

4.1.1. Определение версии СПО ВП

4.1.1.1. Версию установленного СПО ВП можно узнать через Web-интерфейс или при помощи CLI.

4.1.1.2. Определить версию установленного СПО ВП в Web-интерфейсе контроллера можно одним из нескольких способов:

1) в правом нижнем углу Web-интерфейса указана версия СПО ВП;

2) перейти в раздел «Настройки» – «Контроллер» основного меню, далее выбрать пункт «ПО и Сервисы» – «ПО». В открывшемся окне будут указаны версия контроллера СПО ВП и версии основных модулей;

3) перейти в раздел «Серверы» основного меню, выбрать сервер, для которого необходимо узнать версию СПО ВП, далее перейти в пункт «ПО и Сервисы» – «ПО». В открывшемся окне будет указаны версия СПО ВП и версии основных модулей.

4.1.1.3. Чтобы определить версию СПО ВП в Web-интерфейсе узла (ноды), необходимо перейти в раздел «Версия ПО» основного меню, и в открывшемся окне будут указаны версия СПО ВП и версии основных модулей.

4.1.1.4. Определить версию СПО ВП в CLI можно выполнив команду

version

В результате выполнения данной команды будут указаны версия контроллера СПО ВП и версии основных модулей.

4.1.2. Механизм обновления СПО ВП

4.1.2.1. Во время обновления СПО ВП выполняются следующие действия:

– блокируется Web-интерфейс;

– если происходит обновление контроллера, то останавливаются все сервисы. В том числе перестают работать «Высокая доступность» и «Динамическое распределение ресурсов» между серверами;

– обновляется пакетная база СПО ВП;

– происходит автотестирование системы;

– если происходит обновление контроллера, то запускаются все сервисы. «Высокая доступность» и «Динамическое распределение ресурсов» работают в штатном режиме;

– возобновляется штатная работа Web-интерфейса СПО ВП.

4.1.3. Безопасность обновлений

4.1.3.1. Для обеспечения безопасности используется проверка целостности пакетов в репозиториях СПО ВП на основе хеш-суммы, а файл, содержащий контрольные суммы, подписан закрытым ключом с алгоритмом шифрования RSA-4096. При обновлении производится сверка хеш-сумм и проверка подписи с использованием открытого ключа, который поставляется в комплекте с СПО ВП. Таким образом, при повреждении пакета или его подмены установка выполнена не будет.

4.2. Процесс обновления СПО ВП

4.2.1. Существует два варианта обновления:

– с помощью диска;

– по сети.

4.2.2. Для выполнения обновлений с диска необходимо:

– вставить диск с обновлениями в привод DVD-ROM;

– в CLI узла или контроллера выполнить команду

shell

– примонтировать диск командой

mount /dev/cdrom /mnt/

– скопировать содержимое диска командой

cp -r /mnt /var/repo/cdrom

– открыть в редакторе «nano» файл «/etc/apt/sources.list.d/ecp-veil.list» командой

nano /etc/apt/sources.list.d/ecp-veil.list

и заменить содержимое на

rpm file:/var/repo/cdrom/build e2kv6 build

– обновить список пакетов командой

apt-get update

– выполнить обновление командой

apt-get upgrade

– размонтировать диск командой

umount /dev/cdrom

– извлечь диск с обновлениями;

4.2.3. Для выполнения обновлений по сети необходимо:

– в CLI узла или контроллера выполнить команду

shell

– открыть в редакторе «nano» файл «/etc/apt/sources.list.d/ecp-veil.list» командой

nano /etc/apt/sources.list.d/ecp-veil.list

и заменить содержимое файла на полученное от дистрибьютера, примерный вид

rpm http://spacevm.ru/repo/ksoub/build/ e2kv6 build

– обновить список пакетов командой

apt-get update

– выполнить обновление командой

apt-get upgrade

5. ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА СПО ВП

5.1.1. Вход в систему

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

5.1.1.2. При открытии интерфейса управления в браузере откроется окно авторизации, в котором необходимо ввести:

– имя пользователя, «по умолчанию» – admin;

– пароль, «по умолчанию» – veil;

– выбрать язык интерфейса.

5.1.2. Пользователи и роли

5.1.2.1. Управление параметрами собственной учетной записи производится в разделе «Безопасность» – «Пользователи» или справа вверху при нажатии на профиль пользователя. Для просмотра информации о пользователе необходимо нажать на имя пользователя в списке.

5.1.2.2. Если пользователь является администратором, то ему будет доступно управление учетными записями других пользователей в разделе «Безопасность» – «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.

Примечание. Пользователь не удаляется при изменении статуса на «Неактивный». Это сделано для сохранения истории.

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

– «администратор»;

– «администратор безопасности»;

– «оператор ВМ»;

– «только чтение».

Для пользователя со встроенной учетной записью администратора «admin» применяются роли «администратор» и «администратор безопасности». Для него доступны все настройки кластера.

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

Для пользователя с ролью «администратор» действует разрешение – полный доступ, кроме разрешений «администратора безопасности».

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

– управление службами каталогов;

– управление SSL-сертификатами;

– управление пользователями.

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

– управление ресурсами размещения ВМ;

– управление пулами данных;

– управление ВМ, владельцем которых он является.

Для пользователя с ролью «только чтение» действует ограничение – чтение всех параметров кластера, кроме параметров и информации безопасности.

Подробное описание разграничения доступа ролей пользователей приведено в руководстве оператора РАМГ.46653-03 34 01.

5.1.3. Службы каталогов

5.1.3.1. В системе реализована поддержка авторизации пользователей из Windows Active Directory (AD) и FreeIPA посредством Lightweight Directory Access Protocol (LDAP).

Для регистрации внешних пользователей необходимо в разделе «Безопасность» – «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 БД пользователей для Windows AD допускается назначать пользователю или группе роль «суперпользователя».

5.1.3.2. В системе реализована поддержка технологии Single Sign-On (SSO). Для ее 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) СПО ВП;

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

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

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

– параметры пользователя AD (имя пользователя и пароль);

– доменное имя контроллера СПО ВП (субдомен).

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

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

6. НАСТРОЙКА ОТКАЗОУСТОЙЧИВОСТИ

6.1.1. 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 ее 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.

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

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

6.1.4. Интервал перезапуска – это пауза (в секундах), применяемая между попытками перезапуска ВМ.

6.1.5. Высокая доступность – включение ВД для всего кластера будет означать, что для всех ВМ, параметры которых позволяют применить к ним ВД, будет активирована данная опция.

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

6.1.7. 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.

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

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

6.1.10. Процедура добавления серверов в состав кластера подробно описана в разделе 3 руководства оператора РАМГ.46653-03 34 01.

7. РЕЗЕРВНОЕ КОПИРОВАНИЕ БД КОНТРОЛЛЕРА

В БД контроллера содержится конфигурация СПО ВП, включая пользователей и их настройки, информацию о виртуальных машинах, подключенных серверах и систем хранения данных, сетевые настройки как физических подключений, так и виртуальных сетей, и другие.

Повреждение БД может вызвать необратимые последствия, поэтому СПО ВП поддерживает контроль целостности БД, резервное копирование БД и восстановление БД из резервной копии.

7.1. Статистика БД

7.1.1. Для анализа статистики БД контроллера необходимо в CLI выполнить команду

controller db_stats

7.2. Проверка целостности БД

7.2.1. Для проверки целостности БД контроллера необходимо в CLI выполнить команду

controller db_check

В случае повреждения БД система обнаружит поврежденные или отсутствующие файлы.

7.3. Создание резервной копии БД

7.3.1. Создание резервной копии БД контроллера выполняется командой

controller backupdb_create

ВНИМАНИЕ! Создание резервной копии БД перезаписывает резервную копию БД, сделанную ранее.

7.4. Восстановление БД из резервной копии

7.4.1. Восстановление БД контроллера из резервной копии выполняется командой

controller backupdb_restore

7.5. Проверка наличия резервной копии БД

7.5.1. Для проверки наличия резервной копии БД используется команда *controller backupdb_list*

8. СТАТИСТИКА И ЖУРНАЛИРОВАНИЕ СЕРВЕРОВ

8.1. Стек статистики

8.1.1. Общая информация

8.1.1.1. Сбор статистики осуществляется с помощью ПО «prometheus». На контроллере находится центральный сервис «prometheus», который собирает метрики с сервисов «node_exporter» и «domain_exporter» с каждого узла.

Примечание. На основе сбора статистики работают сервисы распределения ВМ по узлам, то есть выбор узлов для создания, миграции, восстановления ВМ, поэтому при отказе сервисов данные операции, возможно, будут недоступны.

8.1.1.2. Для проверки статуса сервисов в CLI есть следующие команды:

1) проверка статуса прометеуса на контроллере (сервис «controller-statistics») выполняется командой CLI *services list*;

2) проверка статуса прометеуса на узле (сервис «node-statistics») выполняется командой CLI *services list*;

3) проверка базы прометеуса на контроллере (сервис «controller-statistics») выполняется командой CLI

system statistics [list|clear|reload|set_storage_time|service]

8.1.1.3. Используются следующие порты сервисов:

– центральный прометеус на контроллере – порт «9090»;

– прометеус статистики узла – порт «9100»;

– прометеус статистики ВМ – порт «9177»;

– Grafana – порт «3000».

8.1.1.4. Каталог хранения статистики на контроллере «/var/log/prometheus/metrics2».

8.1.1.5. Запуск (останов) Web-интерфейса Grafana (работа с графиками) на контроллере выполняется командами CLI

grafana [start|stop]

Базовые логин/пароль – «admin»/«admin».

Порт – «3000».

8.1.1.6. Управление временем хранения статистики узлов на контроллере выполняется командой CLI

system statistics set_storage_time

Базовое значение составляет 360 часов (15 дней).

8.1.2. Расчет размера каталога статистики на контроллере

8.1.2.1. Расчет размера каталога статистики на контроллере приведен ниже. Один вычислительный узел (ВУ) за 1 день при штатной работе условно займет 150 Мбайт.

Примеры расчета:

1) для 20 ВУ с временем хранения 168 часов (7 дней) каталог будет занимать примерно 21 Гбайт;

2) для пяти ВУ с временем хранения 360 часов (15 дней) каталог будет занимать примерно 11,2 Гбайт;

3) для 30 ВУ с временем хранения 30 дней каталог будет занимать примерно 135 Гбайт.

Итого примерный размер каталога равен

*150 Мбайт * количество ВУ * количество дней*

8.2. Стек журналирования

8.2.1. Общая информация

8.2.1.1. Сбор журналов осуществляется с помощью комплекта ПО «td-agent» + «elasticsearch» + «Kibana». На контроллере находится центральный сервис «elasticsearch», который собирает журналы с сервисов «td-agent» с каждого узла. Сервис «td-agent» в свою очередь собирает журналы CLI, супервизора узла, Web-сервиса узла, супервизора контроллера, Web-сервиса контроллера, системные журналы.

«Kibana» служит для удобного просмотра в одном месте всех журналов всех узлов. Подробности смотрите в руководстве оператора РАМГ.46653-03 34 01.

8.2.1.2. Для проверки статуса сервисов в CLI есть следующие команды:

1) проверка статуса «elasticsearch» (сервис «controller-logger») на контроллере выполняется командой CLI *services list*;

2) проверка статуса «td-agent» на узле выполняется командой CLI *services list*;

3) отдельно в Web-интерфейсе выведена кнопка редиректа (перенаправление) на сервис «Kibana», находящийся на контроллере. «По умолчанию» сервис выключен, а включить (выключить) его можно в CLI командой *kibana start|stop*. «Kibana» позволяет удобно просматривать и фильтровать все журналы системы. Подробности настройки и фильтрации смотрите на официальном сайте «Kibana».

8.2.1.3. Каталогом хранения журналов на контроллере является «/var/log/elasticsearch-data».

8.2.1.4. Управление временем хранения журналов узлов на контроллере выполняется командой CLI

system logging [get_days2keep|set_days2keep]

Базовое значение составляет 30 дней.

8.2.2. Расчет размера каталога журналов узлов на контроллере

8.2.2.1. Расчет размера каталога журналов узлов на контроллере приведен ниже. Один ВУ за 1 день при штатной работе условно займет 200 Мбайт.

Примеры расчета:

1) для 20 ВУ с временем хранения 7 дней каталог будет занимать примерно 28 Гбайт;

2) для пяти ВУ с временем хранения 30 дней каталог будет занимать примерно 30 Гбайт;

3) для 30 ВУ с временем хранения 30 дней каталог будет занимать примерно 180 Гбайт.

Итого примерный размер каталога равен

*200 Мбайт * количество ВУ * количество дней*

8.2.3. Очистка журналов «elasticsearch»

8.2.3.1. Очистка журналов «elasticsearch» на контроллере выполняется командой CLI

system logging clear

8.3. Состав каталога журналов

8.3.1. Общая информация

8.3.1.1. Каталог журналов расположен в «*/var/log».* «По умолчанию» под каталог журналов при установке выделяется 80 Гбайт.

Примечание. Журналы на контроллере и узлах автоматически ротируются.

8.3.1.2. Каталог журналов состоит из:

– журналы всех узлов (только на контроллере). Подробное описание приведено в разделе 8.2 данного руководства;

– статистика всех узлов (только на контроллере). Подробное описание приведено в разделе 8.1 данного руководства;

– журналы сервисов узла – «/var/log/»;

– журналы дампов крахов процессов – «/var/log/crash/»;

– журналы общих сервисов – «/var/log/veil/»;

– журналы CLI – «/var/log/veil/cli/»;

– журналы супервизора узла – «/var/log/veil/node/»;

– журналы супервизора контроллера (только на контроллере) – «/var/log/veil/controller/»;

– резервная копия базы данных контроллера (только на контроллере) – «/var/log/veil/controller/db_backup/»;

– архивы журнала контроллера (только на контроллере) – «/var/log/veil/controller/journal/».

8.3.2. Расчет размера каталога журналов на контроллере

8.3.2.1. Сильно зависящими от размера инфраструктуры и времени хранения являются размеры каталога журналов всех узлов и статистики всех узлов.

Базовый размер каталога журналов «/var/log» в режиме установки «Preceed» равен 80 Гбайт. Оставляем 10 Гбайт под журналы сервисов СПО ВП и системные, остается 70 Гбайт.

Условный расчет выполняется следующим образом:

*150 Мбайт * количество серверов * 15 дней + 200 Мбайт * количество серверов * 30 дней = 8250 Мбайт * количество серверов*

Имея 70 Гбайт, получаем 8 серверов.

В итоге места «по умолчанию» хватит на 8 серверов на 15 дней хранения статистики и 30 дней хранения журналов.

Общая условная формула для расчета следующая:

*(количество серверов * количество дней * 350 Мбайт + 10 000 Мбайт)/1000*

8.3.3. Возможные действия при переполнении каталога журналов

8.3.3.1. Ниже приведены возможные действия при переполнении каталога журналов:

– проверить вывод команды с помощью *df -h;*

– запустить в CLI команду *log remove_archives*, которая удалит все архивы «.gz»;

– запустить в CLI команду *ncdu /var/log/* (с версии 4.6.2), найти и очистить самые крупные файлы с помощью команды *> /var/log/syslog*.

– уменьшить на будущее время хранения статистики;

– уменьшить на будущее время хранения журналов;

– очистить хранилище журналов командой CLI *system logging clear*;

– возможно, для корректной работы потребуется перезапустить часть сервисов – «redis», «controller-db (postgresql)», «node-engine», «controller-engine»;

– запустить в CLI команду *system autotest.*

Принудительно ротировать файлы журналов можно командой *log rotate*.

8.3.4. Причины возможного переполнения раздела журналов

8.3.4.1. Желательно перед очисткой разобраться, почему переполнились журналы, и принять меры по донастройке систем журналирования и ротирования или устранению причины генерации большого количества журналов.

8.3.4.2. Возможные причины:

– увеличилось количество узлов, и, соответственно, размер журналируемых данных на контроллере. Рекомендуется уменьшить количество времени хранения журналов «elasticsearch» с помощью команды

system logging [get_days2keep|set_days2keep]

– увеличилось количество узлов, и, соответственно, размер собираемой статистики на контроллере.

Рекомендуется уменьшить количество времени хранения статистики «prometheus» с помощью команды

system statistics [set_storage_time]

– какое-то ПО постоянно журналирует ошибки. Это может быть, как прикладное ПО, так и ошибки оборудования, например, BMC платы или процессора. Необходимо локализовать сервис, посмотрев, какой файл журналов заполняется или syslog, и принять меры по устранению (самим или написать в техподдержку).

9. АВАРИЙНЫЙ РЕЖИМ СПО ВП

9.1. Аварийный режим – это режим, который используется для восстановления системы и исправлений последствий непредвиденных сбоев. В «Аварийном режиме» становятся доступны некоторые отладочные функции, недоступные в обычном режиме.

ВНИМАНИЕ! Стоит с особой осторожностью использовать «Аварийный режим»!

9.2. Для того чтобы перейти в «Аварийный режим», необходимо в CLI узла или контроллера выполнить команду *shell*.

Чтобы выйти из «Аварийного режима» необходимо выполнить команду *exit* или нажать сочетание клавиш «Ctrl+D».

10. ПРОВЕРКА ПРОГРАММЫ

10.1. Самотестирование программы

10.1.1. При включении серверной платформы автоматически запускается СПО ВП и начинается процедура самотестирования, при этом осуществляются проверки целостности файловой системы.

10.2. Результаты тестирования

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

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

10.2.3. 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.

11. УДАЛЕННОЕ УПРАВЛЕНИЕ СЕРВЕРОМ

11.1. При наличии на сервере разъема последовательного порта номер 2 (ttyS1, COM2, 115200 бит/с, 8n1) в СПО ВП предусмотрена возможность работы через этот порт посредством подключения через нуль-модемный кабель с рабочей станции.

11.2. При наличии поддержки аппаратурой сервера протокола IPMI Serial-over-Lan (SoL) возможно удаленное управление сервером.

11.3. Пример включения SoL в BIOS сервера приведен на рис. 4.

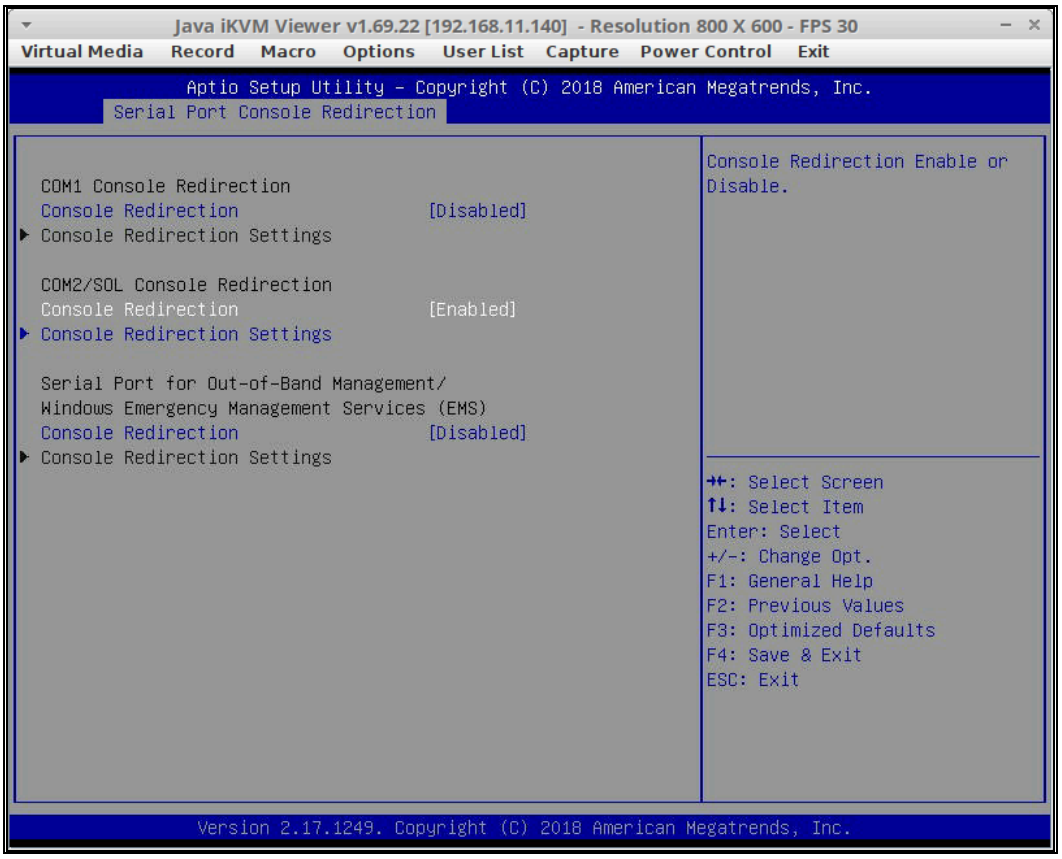

Рис. 5

11.4. На клиентской машине устанавливаем утилиту «ipmitools».

11.5. Установка на ОС Ubuntu выполняется командой

sudo apt-get install ipmitool

11.6. Пример команды проверки текущего статуса питания сервера

ipmitool -H 192.168.99.1 -U ADMIN -P 4a23t887UP -I lanplus chassis power status

11.7. Пример команды рабочего терминала

ipmitool -H 192.168.99.1 -U ADMIN -P 4a23t887UP -I lanplus sol activate

12. ИСПОЛЬЗУЕМЫЕ СИСТЕМОЙ ПОРТЫ

12.1. В таблице 7 приведены используемые внутренними сервисами порты.

Таблица 7

Порт	Применение
80	Web-интерфейс (http)
443	Web-интерфейс (https)
9090	Шина статистики (Prometheus на контроллере)
9100	Шина статистики (Prometheus статистики узла на узле)
9177	Шина статистики (Prometheus статистики ВМ на узле)
3000	Шина статистики (GRAFANA)
6379	REDIS
11300	Шина обмена статусами хранилищ, сети и ВМ между узлами и контроллером
22	SSH
46003	Шина heartbeat, постановки и проверки выполнения задач между узлами и контроллером
24224	Шина логирования (FLUENTD)
9200, 9300	Шина логирования (ELASTICSEARCH)
9000, 9001(ssl)	Шина логирования (KIBANA)
5404, 5405, 5406	GFS2 (corosync) кластерный транспорт
7777	OCFS2 кластерный транспорт
24007-24008, 38465-38467, 49152-49199	GLUSTER кластерный транспорт
(TCP,UDP)/111	RPC portmapper (используется GLUSTER)
UDP/123	Сервис синхронизации времени (NTP) на контроллере
UDP/161,162	SNMP
9400, 9401	Объектное S3 хранилище (MinIO)

13. СООБЩЕНИЯ СИСТЕМНОМУ ПРОГРАММИСТУ

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

13.2. Подсказка по командам CLI-интерфейса вызывается командой

help

ПРИЛОЖЕНИЕ 1

ПРОЦЕДУРА УСТАНОВКИ ОС «АЛЬТ СЕРВЕР 10.1 ДЛЯ ЭЛЬБРУС»

Перед началом установки необходимо подготовить установочный CD/DVD-диск «Альт Сервер 10.1 для Эльбрус». Это можно сделать самостоятельно, записав ISO-образ дистрибутива на CD/DVD.

Примечания:

1. Получить ISO-образ ОС «Альт Сервер 10.1 для Эльбрус» можно по запросу у предпрятия-разработчика ОС, его официального представителя или вендора.

2. Ознакомится с документацией разработчика можно на его официальном сайте по ссылке

https://docs.altlinux.org/ru-RU/alt-server-e2k/10.0/html/alt-server-e2k/index.html.

1. Начало установки

1.1. Загрузить компьютер с помощью загрузочного носителя, находящегося на установочном DVD-диске с дистрибутивом (система должна поддерживать загрузку с устройства для чтения DVD).

1.2. После включения аппаратной платформы «Эльбрус» происходит инициализация программы начальной загрузки, в процессе которой есть возможность вмешательства после вывода следующей строки:

Autoboot in 03 sec. PRESS SPACE TO DISABLE IT.

Необходимо нажать «пробел», после чего должны появиться следующие строки:

Key pressed. Autoboot canceled.

CPU#00: Starting menu.

BOOT SETUP

Press command letter, or press 'h' to get help

:

1.3. Можно запросить подсказку нажатием клавиши «h», но необходимыми являются следующие команды:

– d – show Disks and partitions (показать диски и разделы);

– c – Change boot parameters (изменить параметры загрузки);

– u – show cUrrent parameters (показать текущие параметры);

– m – save params to NVRAM (сохранить параметры в NVRAM);

– b – start Boot.conf menu (запустить меню Boot.conf).

1.4. При нажатии на клавишу «d» выводится список дисков:

:d

CPU#00: Drive [2]: SATA - PCI BUS[1]:DEV[3]:FUNC[0], MCST SATA COMBINED Port

[0] - KINGSTON SMS200S3120G

CPU#00: Partition [0]: Linux EXT2;

U:246194e7-0512-4db3-a821-cbcbe3c92c38 L:""

CPU#00: Partition [1]: Linux swap

CPU#00: Partition [3]: Extended

CPU#00: Partition [4]: Unknown file system type

CPU#00: Drive [10]: ATAPI device

1.5. В данном случае идентификатор «10» присвоен внешнему USB DVD-приводу, с которого и будет произведена установка ОС. Следует выбрать его, указав идентификатор «10» ответом на первый вопрос команды «c» и нажав клавишу «Esc» на остальные вопросы:

:c

CHANGE BOOT PARAMETERS

Current Settings:

drive_number: '2'

drive label: ''*

partition_number: '0'

file system id: '07bde958-ec62-492e-933c-17334bb02da2'

command_string: ''

filename: ''

initrdfilename: ''

autoboot in: '10'

To advance to next setting press ENTER. To skip setting press ESC

Enter drive number : 10

Enter partition number: < Skipped >

Enter command string : < Skipped >

Enter filename : < Skipped >

Enter initrd file name: < Skipped >

Enter autoboot value : < Skipped >

Current Settings:

drive_number: '10'

drive label: ''

partition_number: '0'

file system id: ''

command_string: ''

filename: ''

initrdfilename: ''

autoboot in: '10'

CPU#00: Search drive and partition by label or uuid succeed

1.6. Затем необходимо перейти к загрузке последовательным нажатием клавиш «b» «Tab» «Enter»:

:b

boot# install

CPU#00: Label 'install' found, loading parameters

CPU#00: Search drive and partition by label or uuid succeed

Trying to load and start image with following parameters:

drive_number: '10'

drive label: ''

partition_number: '0'

file system id: ''

command_string: 'hardreset fastboot live automatic=method:cdrom'

filename: '/alt0/vmlinux.0'

initrdfilename: '/alt0/full.cz'

ВНИМАНИЕ! На этом этапе установки графический манипулятор типа «мышь» не поддерживается. Для выбора опций установки и различных вариантов необходимо использовать клавиатуру.

1.7. После загрузки инсталлятора установка продолжается штатным образом.

1.8. После установки системы, если установка производилась на диск, отличного от того, с которого аппаратная платформа загружается «по умолчанию», следует повторно зайти в конфигурацию программы начальной загрузки, определить загрузочный диск, нажав «d» и указать его в качестве загрузочного диска «по умолчанию», нажав «c». После изменений параметров загрузки, следует выполнить команду «m» для записи изменений в NVRAM и их применения в дальнейшем.

2. Последовательность установки

2.1. До того, как будет произведена установка базовой системы на жесткий диск, программа установки работает с образом системы, загруженным в оперативную память компьютера.

2.2. Если инициализация оборудования завершилась успешно, то будет запущен графический интерфейс программы-установщика.

2.3. Процесс установки разделен на шаги. Каждый шаг посвящен настройке или установке определенного свойства системы. Шаги нужно проходить последовательно. Переход к следующему шагу происходит по нажатию кнопки «Далее». При помощи кнопки «Назад» (при необходимости) можно вернуться к уже пройденному шагу и изменить настройки. Однако, возможность перехода к предыдущему шагу ограничена теми шагами, в которых нет зависимости от данных, введенных ранее.

Если по каким-то причинам возникла необходимость прекратить установку, необходимо нажать кнопку «Reset» на корпусе системного блока компьютера.

Примечание. В случае необходимости можно безопасно прервать установку только до шага «Подготовка диска», поскольку до этого момента не производится никаких изменений на жестком диске.

Технические сведения о ходе установки можно посмотреть, нажав «Ctrl»+«Alt»+«F1».

Вернуться к программе установки – «Ctrl»+«Alt»+«F7».

Открыть отладочную виртуальную консоль – «Ctrl+«Alt+«F2».

Каждый шаг сопровождается краткой справкой, которую можно вызвать, нажав кнопку «Справка» или клавишу «F1».

2.4. Во время установки системы выполняются следующие шаги настройки:

– язык;

– дата и время;

– подготовка диска;

– установка системы;

– сохранение настроек;

– настройка сети;

– администратор системы;

– системный пользователь;

– завершение установки.

3. Язык

3.1. Установка «Альт Сервер 10.1 для Эльбрус» начинается с выбора основного языка – языка интерфейса программы установки и устанавливаемой системы (рис. 1.1). Необходимо выбрать «Русский».

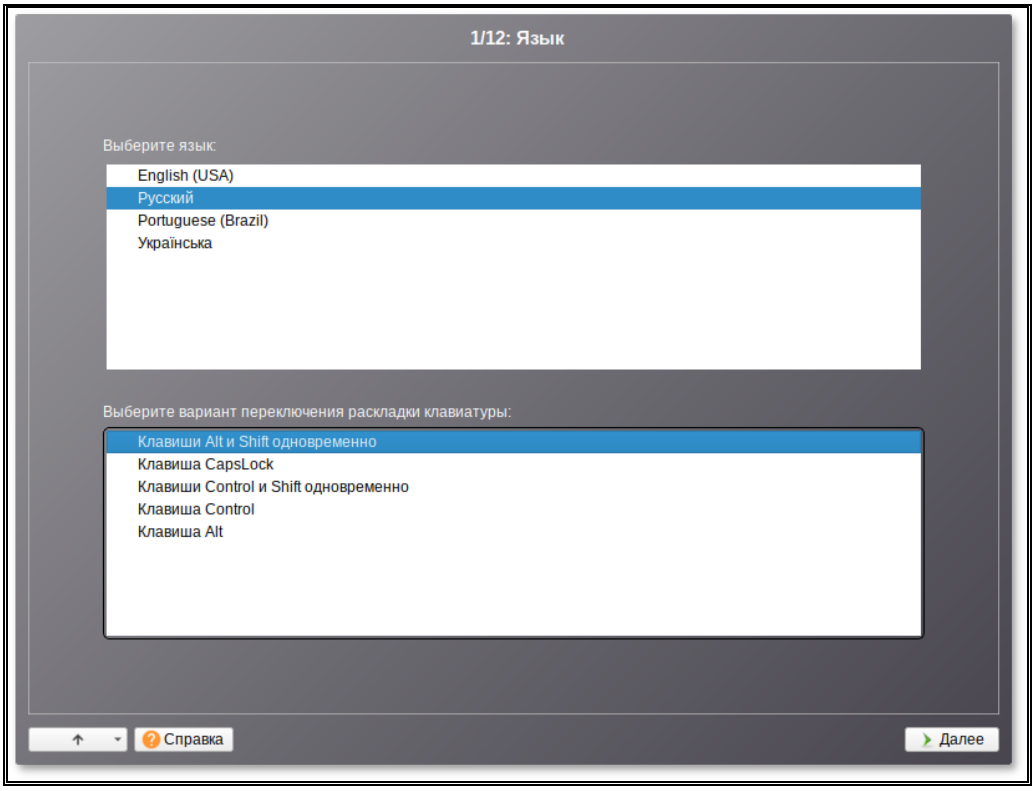

Рис. 1.1

3.2. На этом же этапе выбирается вариант переключения раскладки клавиатуры. Раскладка клавиатуры – это привязка букв, цифр и специальных символов к клавишам на клавиатуре. Необходимо выбрать «Клавиши «Alt»+«Shift» одновременно».

4. Дата и время

4.1. На данном этапе выполняется выбор страны и города, по которым будет определен часовой пояс и установлены системные часы (рис. 1.2). Необходимо выбрать:

– страна – Россия;

– часовой пояс – Москва (+03).

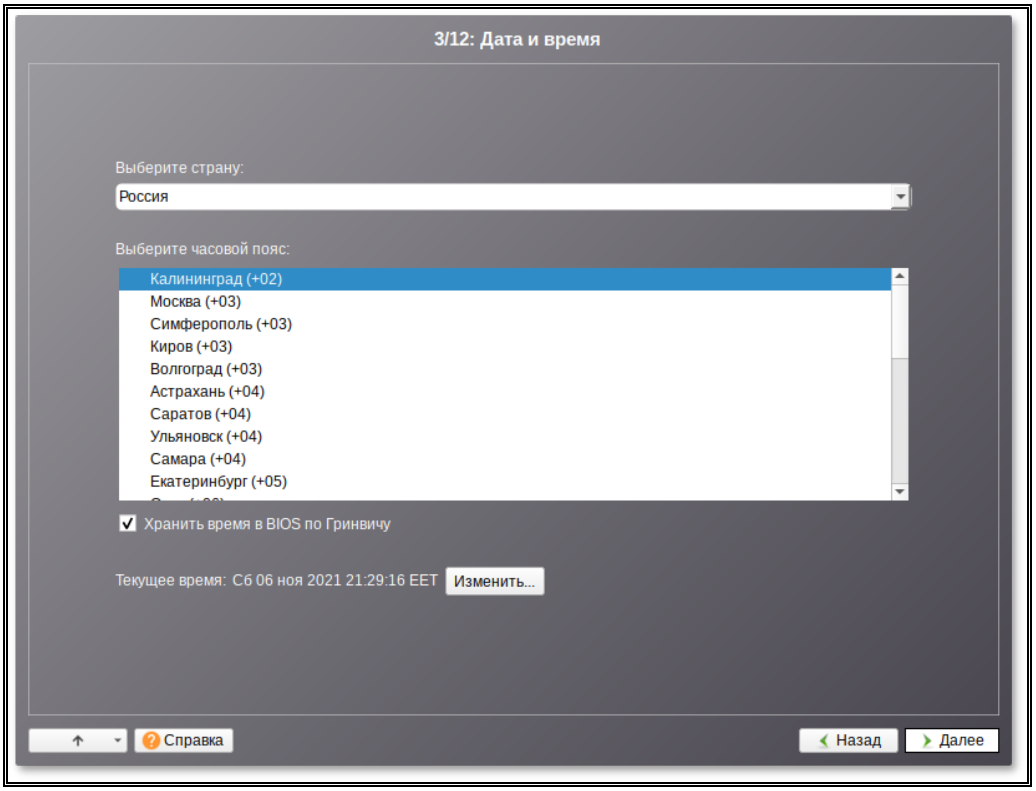

Рис. 1.2

4.2. Пункт «Хранить время в BIOS по Гринвичу» выставляет настройки даты и времени в соответствии с часовыми поясами, установленными по Гринвичу, и добавляет к местному времени часовую поправку для выбранного региона.

4.3. После выбора часового пояса будут предложены системные дата и время «по умолчанию».

4.4. Для ручной установки текущих даты и времени нужно нажать кнопку «Изменить…». Откроется окно ручной настройки системных параметров даты и времени (рис. 1.3).

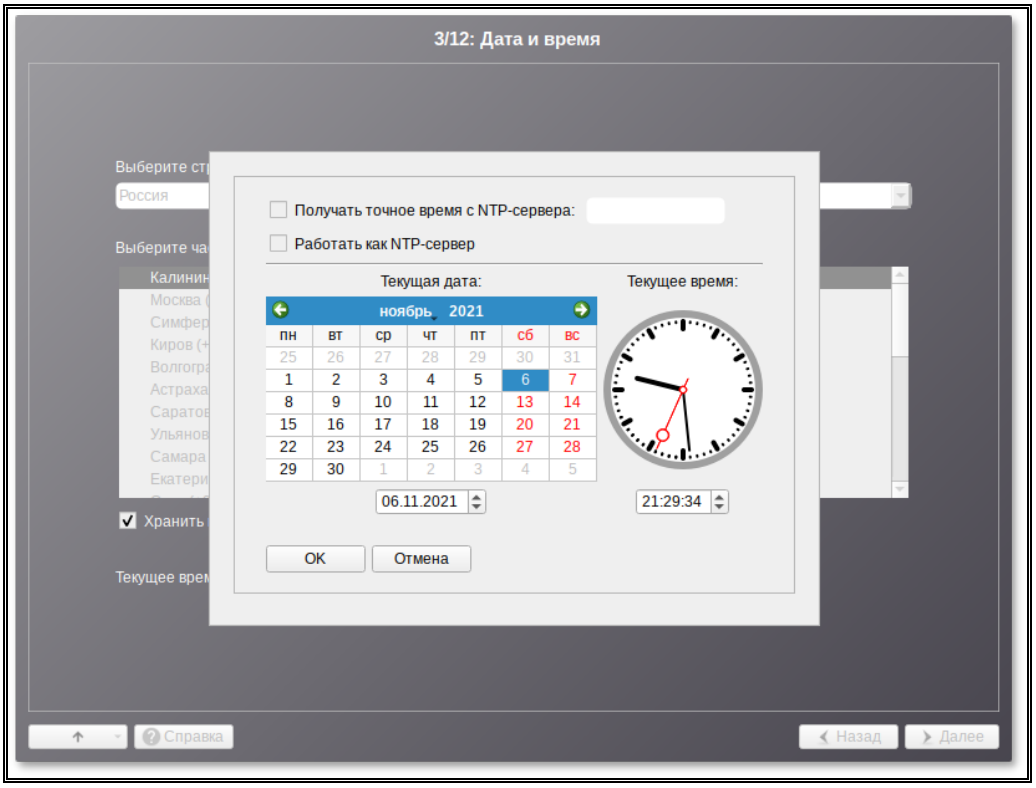

Рис. 1.3

4.5. Для сохранения настроек и продолжения установки системы в окне ручной установки даты и времени необходимо нажать кнопку «ОК» и затем в окне «Дата и время» нажать кнопку «Далее».

5. Подготовка диска

На этом этапе подготавливается площадка для установки «Альт Сервер 10.1 для Эльбрус», в первую очередь выделяется свободное место на диске.

Переход к этому шагу может занять некоторое время. Время ожидания зависит от производительности компьютера, объема жесткого диска, количества разделов на нем и других параметров.

5.1. Выбор профиля разбиения диска

5.1.1. После завершения первичной конфигурации загрузочного носителя откроется окно «Подготовка диска» (рис. 1.4). В списке разделов перечислены уже существующие на жестких дисках разделы (в том числе, здесь могут оказаться съемные flash-диски, подключенные к компьютеру в момент установки).

Необходимо выбрать «sda», «sdb».

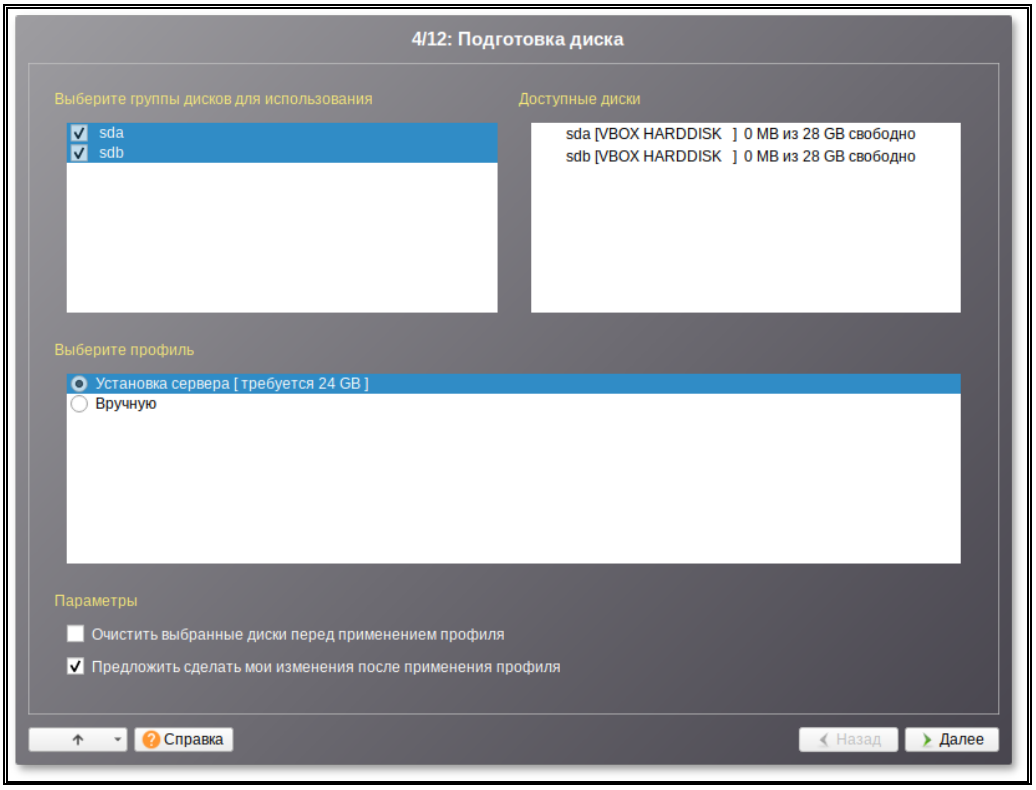

Рис. 1.4

5.1.2. В списке «Выберите профиль» перечислены доступные профили разбиения диска. Профиль – это шаблон распределения места на диске для установки ОС. Можно выбрать один из профилей:

– установка сервера. Профиль предполагает автоматическое разбиение диска;

– вручную.

Необходимо выбрать «Установка сервера» и нажать «Далее».

5.2. Автоматический профиль разбиения диска

ВНИМАНИЕ! Будьте внимательны при использовании автоматического профиля разбиения дисков (рис. 1.5). Соответствующие изменения на диске происходят сразу же по нажатию кнопки «Далее».

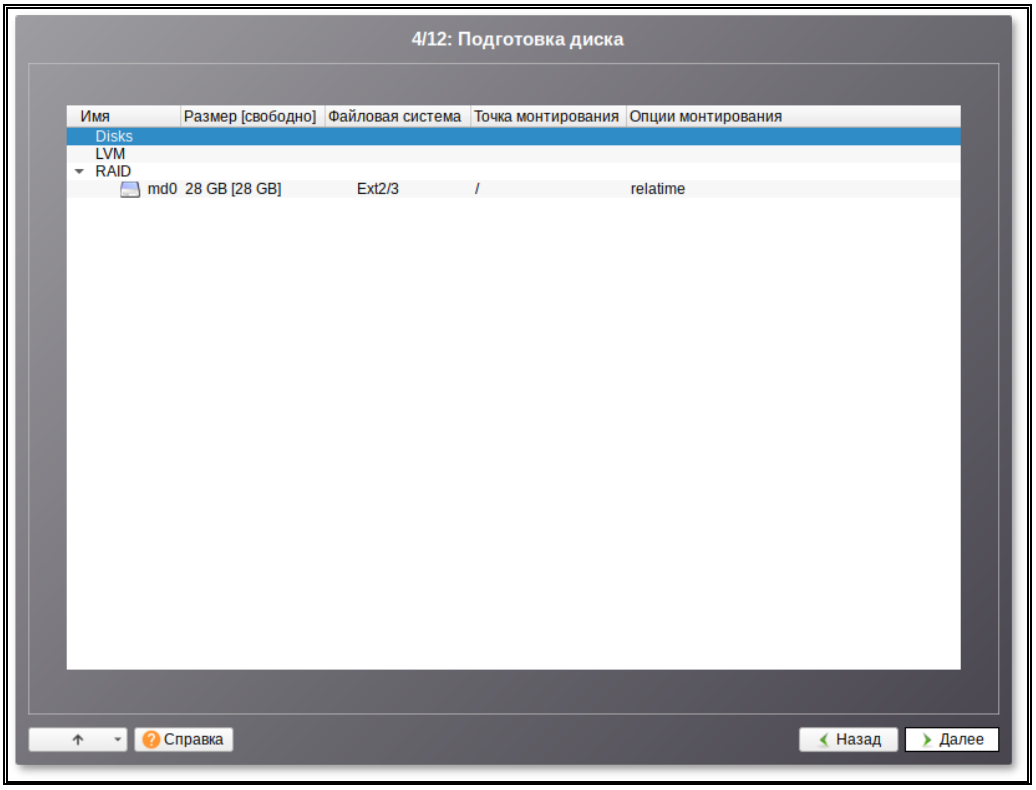

Рис. 1.5

5.2.1. Если при применении профиля автоматического разбиения диска доступного места на диске окажется недостаточно, то на монитор будет выведено сообщение об ошибке – «Невозможно создать все разделы, недостаточно места на диске» (рис. 1.6).

5.2.2. Для решения этой проблемы можно полностью очистить место на диске, отметив пункт «Очистить все диски перед применением профиля» и применить профиль повторно.

5.2.3. Если сообщение о недостатке места на диске появляется и далее при отмеченном пункте «Очистить все диски перед применением профиля», то это связано с недостаточным для использования автоматических методов разметки объемом всего диска. В этом случае можно вернуться назад и воспользоваться методом ручной разметки, выбрав профиль «Вручную».

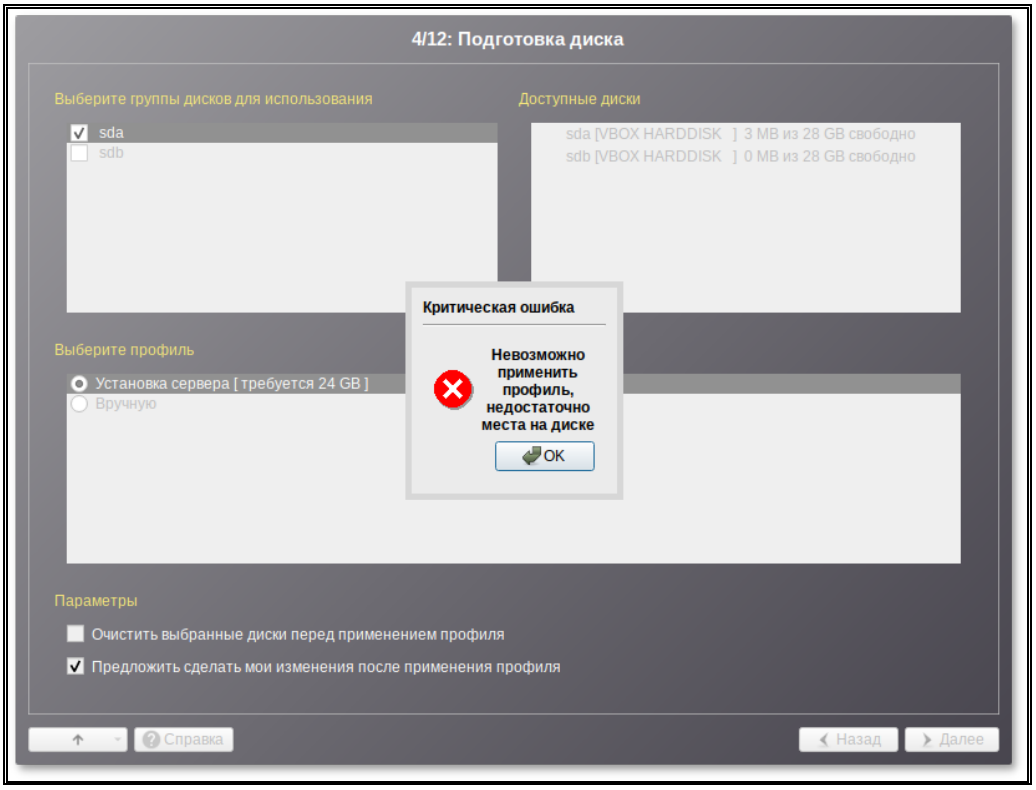

Рис. 1.6

ВНИМАНИЕ! При отмеченном пункте «Очистить все диски перед применением профиля» будут удалены все данные со всех дисков (включая внешние USB-носители) без возможности восстановления. Рекомендуется использовать эту возможность при полной уверенности в том, что диски не содержат никаких ценных данных.

Разбивка не затрагивает CF-диск, на котором может храниться система бинарной трансляции.

5.3. Ручной профиль разбиения диска

5.3.1. При необходимости освободить часть дискового пространства следует воспользоваться профилем разбиения «Вручную». В этом случае можно удалить некоторые из существующих разделов или содержащиеся в них файловые системы. После этого можно создать необходимые разделы самостоятельно или вернуться к шагу выбора профиля и применить автоматический профиль. Выбор этой возможности требует знаний об устройстве диска и технологиях его разметки.

ВНИМАНИЕ! В случае ручной разбивки необходимо создать и подключить на первом разделе диска (не MD RAID) раздел для ядра «/boot» с файловой системой «ext2» (то есть без «extents» и журнала).

5.3.2. По нажатию кнопки «Далее» будет произведена запись новой таблицы разделов на диск и форматирование разделов. Только что созданные на диске программой установки разделы пока не содержат данных и поэтому форматируются без предупреждения. Уже существовавшие, но измененные разделы, которые будут отформатированы, помечаются специальным значком в колонке «Файловая система» слева от названия. При уверенности в том, что подготовка диска завершена, подтвердить переход к следующему шагу нажатием кнопки «Далее».

5.3.3. Не следует форматировать разделы с теми данными, которые пользователь хочет сохранить, например, со старыми пользовательскими данными («/home») или с другими операционными системами. С другой стороны, отформатировать можно любой раздел, который пользователь хочет «очистить» (удалить все данные).

5.4. Дополнительные возможности разбиения диска

5.5. Ручной профиль разбиения диска позволяет установить ОС на программный RAID-массив, разместить разделы в томах LVM и использовать шифрование на разделах. Данные возможности требуют от пользователя понимания принципов функционирования указанных технологий.

5.6. Избыточный массив независимых дисков RAID (Redundant Array of Independent Disks) – технология виртуализации данных, которая объединяет несколько НЖМД в логический элемент для избыточности и повышения производительности.

Примечание. Для создания программного RAID-массива потребуется минимум два жестких диска.

5.7. Программа установки поддерживает создание программных RAID-массивов следующих типов:

– RAID 1;

– RAID 0;

– RAID 4/5/6;

– RAID 10.

5.8. Процесс подготовки к установке на RAID условно можно разбить на следующие шаги:

– создание разделов на жестких дисках;

– создание RAID-массивов на разделах жесткого диска;

– создание файловых систем на RAID-массиве.

5.9. Для настройки параметров нового раздела из состава RAID-массива необходимо выбрать неразмеченный диск в окне профиля разбивки пространства «Подготовить разделы вручную» и нажать кнопку «Создать раздел».

5.10. При создании разделов на жестких дисках для последующего включения их в RAID-массивы следует указать «Тип раздела» – Linux RAID (рис. 1.7).

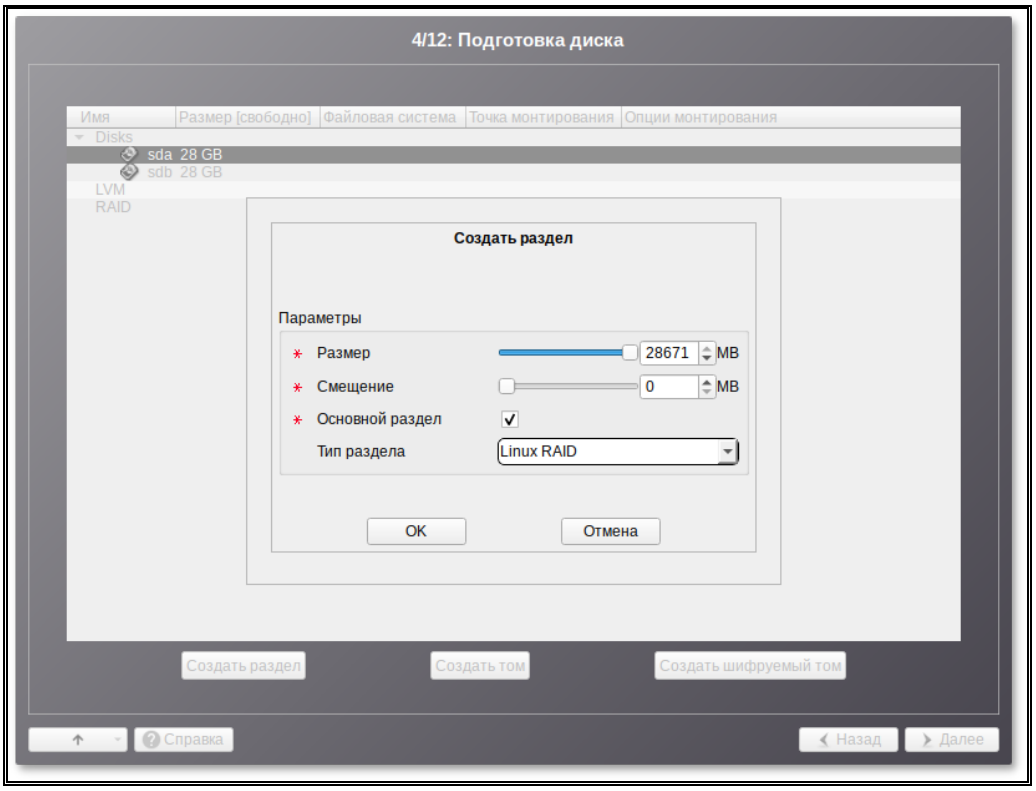

Рис. 1.7

В этом окне необходимо настроить следующие параметры:

– размер – в поле необходимо указать размер будущего раздела (Мбайт);

– смещение – в поле необходимо указать смещение начала данных на диске (Мбайт);

– основной раздел – необходимо отметить этот пункт, если раздел является основным для установки ОС;

– тип раздела – в раскрывающемся списке нужно выбрать значение «Linux RAID» для последующего включения раздела в RAID-массив.

Примечание. При создании разделов следует учесть, что объем результирующего массива может зависеть от размера, включенных в него разделов жесткого диска. Например, при создании RAID 1, результирующий размер массива будет равен размеру минимального участника.

5.11. После создания разделов на дисках можно переходить к организации самих RAID-массивов. Для этого в списке следует выбрать пункт «RAID», после чего нажать кнопку «Создать RAID» (рис. 1.8).

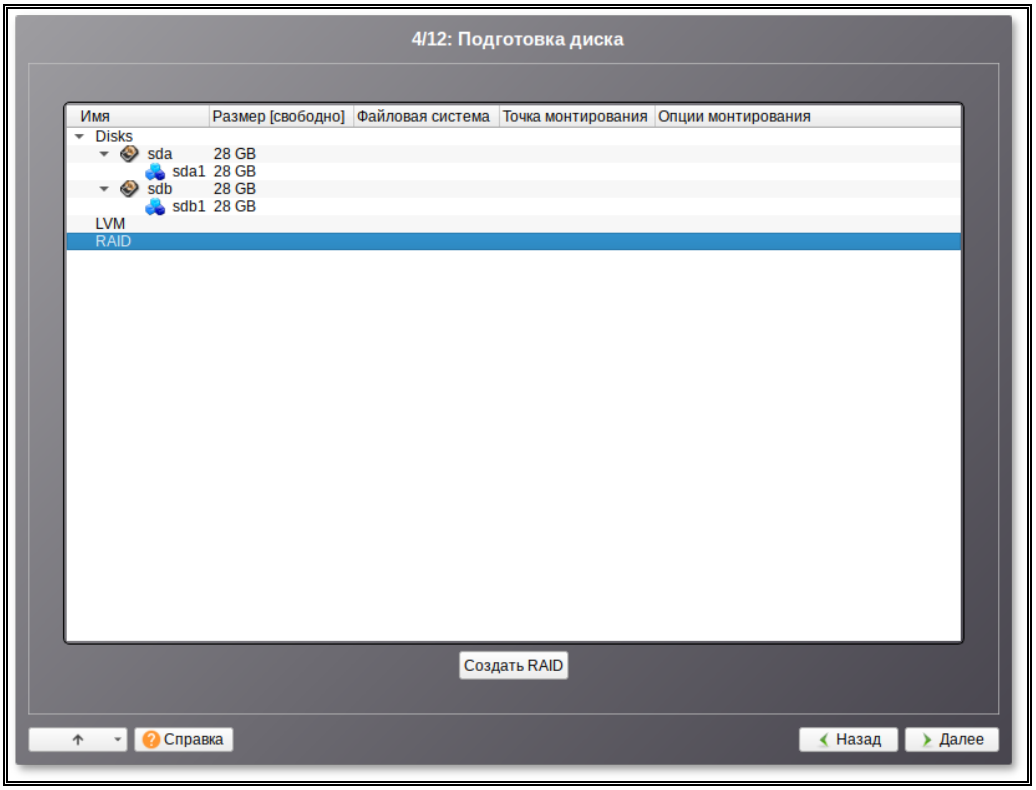

Рис. 1.8

Далее мастер предложит выбрать тип массива (рис. 1.9). Необходимо выбрать «MD-устройство уровня RAID1» и нажать «ОК».

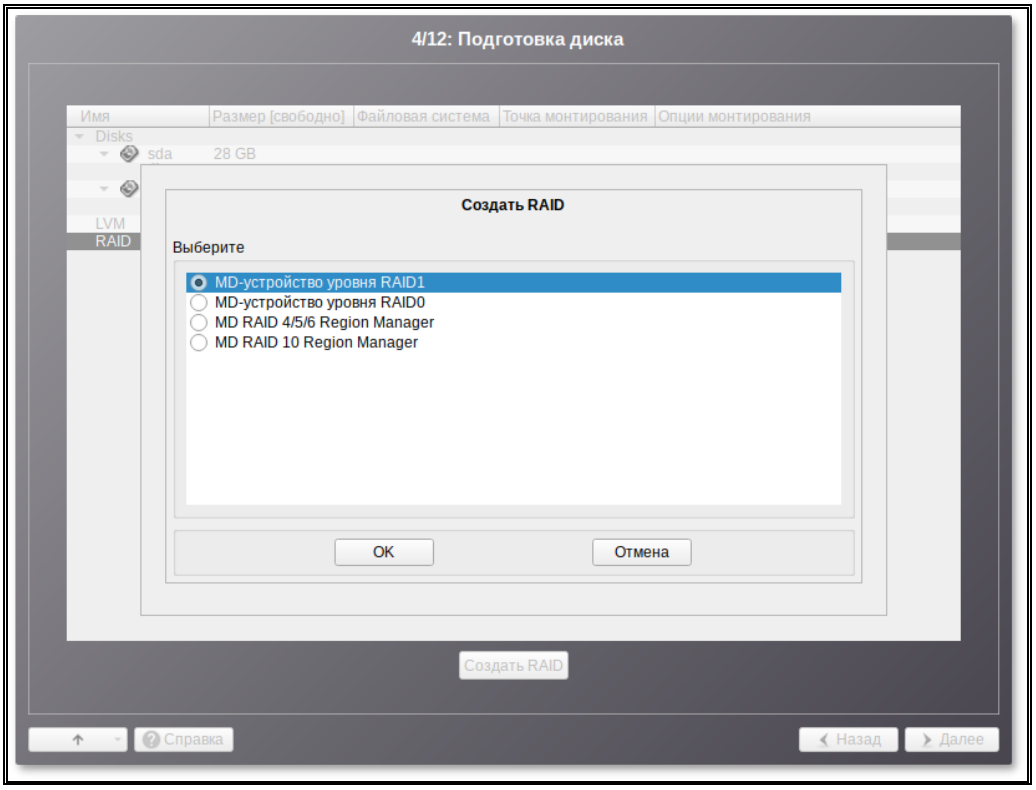

Рис. 1.9

Далее необходимо указать участников RAID-массива (рис. 1.10). Необходимо выбрать «sda1» и «sdb1» и нажать «ОК».

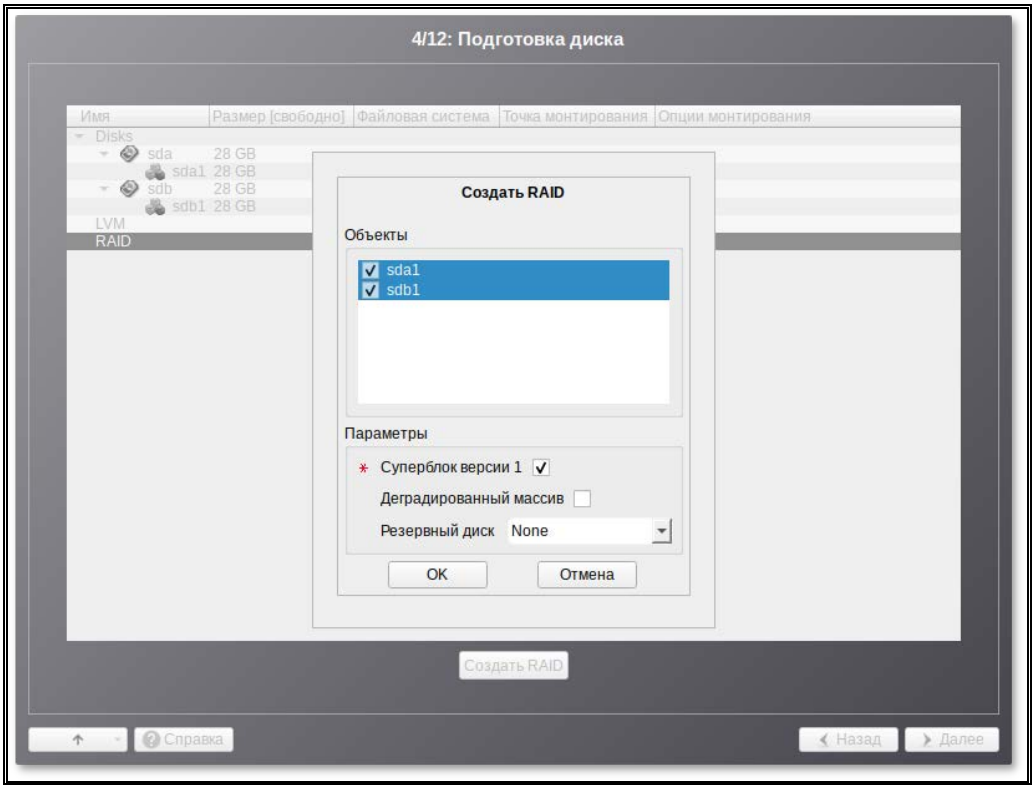

Рис. 1.10

После создания RAID-массивов их можно использовать как обычные разделы на жестких дисках, то есть, на них можно создавать файловые системы или же, например, включать их в LVM-тома.

6. Создание LVM-томов

6.1. Менеджер логических дисков LVM (Logical Volume Manager) – средство гибкого управления дисковым пространством, позволяющее создавать поверх физических разделов (либо неразбитых дисков) логические тома, которые в самой системе будут видны как обычные блочные устройства с данными (обычные разделы).

6.2. Процесс подготовки к установке на LVM условно можно разбить на следующие шаги:

– создание разделов на жестких дисках;

– создание группы томов LVM;

– создание томов LVM;

– создание файловых систем на томах LVM.

ВАЖНО! Для создания группы томов LVM может потребоваться предварительно удалить существующую таблицу разделов с жесткого диска.

6.3. Для настройки параметров нового раздела необходимо выбрать неразмеченный диск в окне профиля разбивки пространства «Подготовить разделы вручную» и нажать кнопку «Создать раздел». При создании разделов на жестких дисках для последующего включения их в LVM-тома следует указать «Тип раздела» – «Linux LVM» (рис. 1.11).

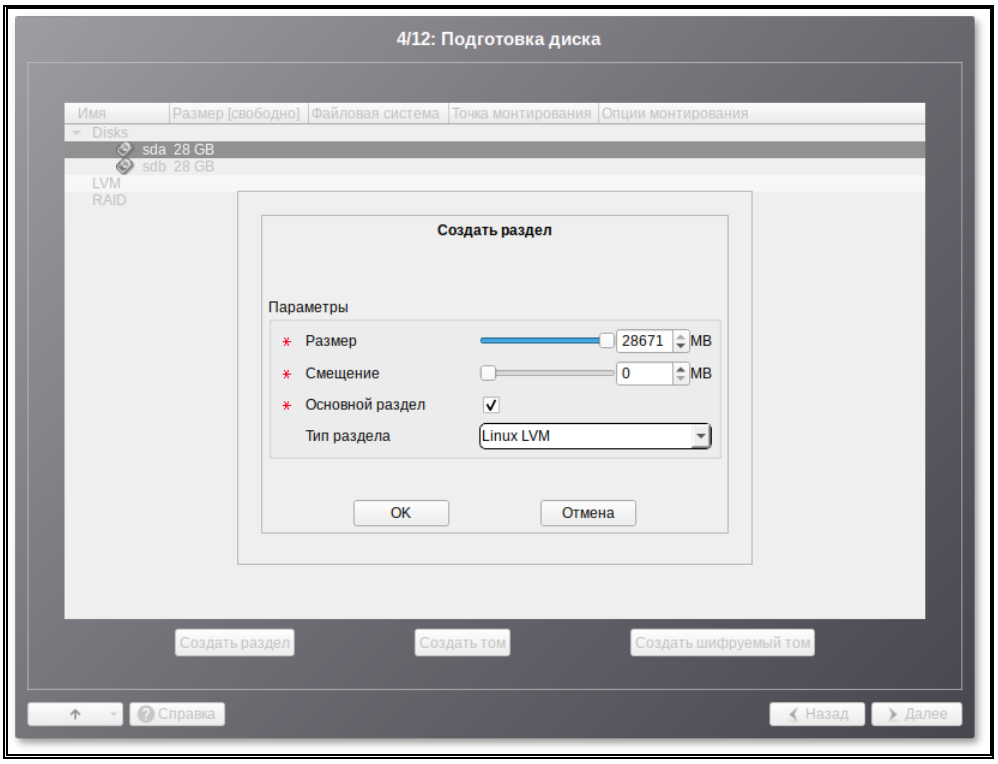

Рис. 1.11

6.4. После создания разделов на дисках можно переходить к созданию группы томов LVM. Для этого в списке следует выбрать пункт «LVM», после чего нажать кнопку «Создать группу томов» (рис. 1.12).

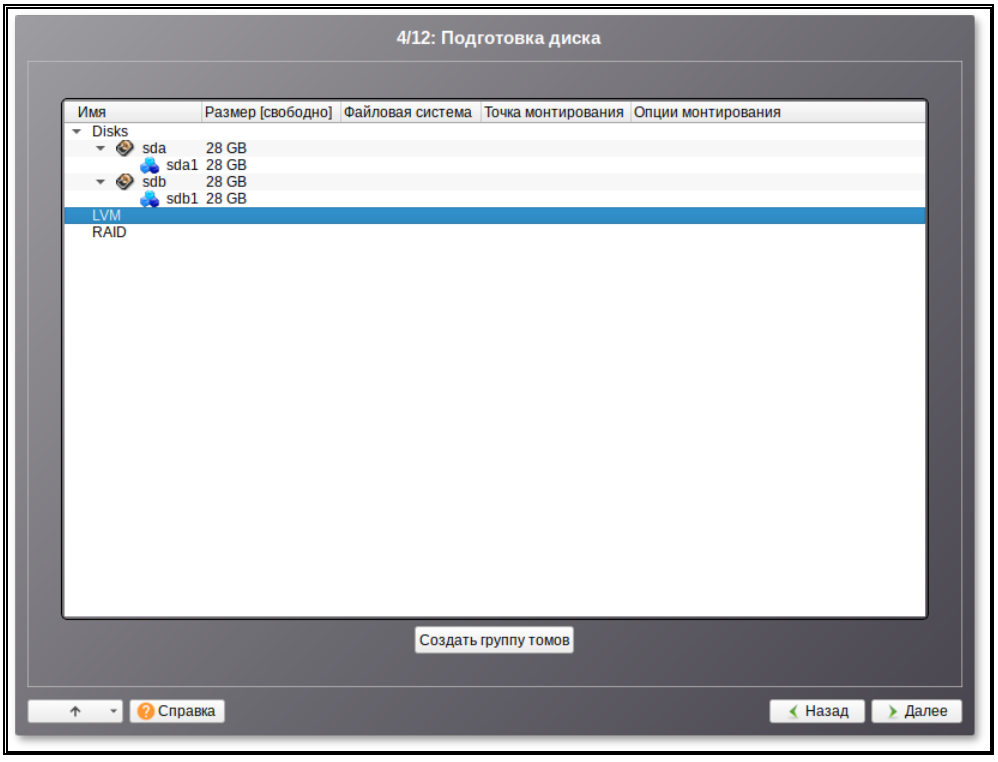

Рис. 1.12

6.5. В открывшемся окне необходимо выбрать разделы «sda1» и «sdb1», которые будут входить в группу томов, указать название группы томов «VolGroup» и выбрать размер экстента (рис. 1.13). После заполнения нажать «ОК».

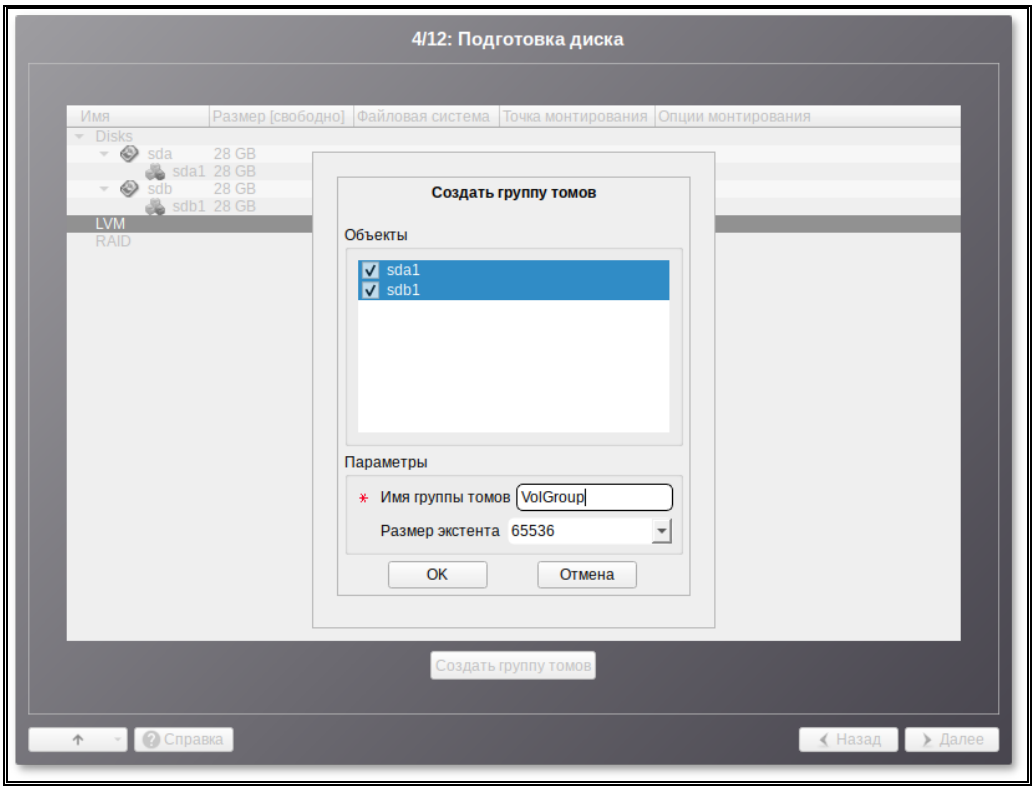

Рис. 1.13

Примечание. Размер экстента представляет собой наименьший объем пространства, который может быть выделен тому. Размер экстента «по умолчанию» 65536 (65536*512 байт = 32 Мб, где 512 байт – размер сектора).

6.6. После создания группы томов LVM ее можно использовать как обычный жесткий диск, то есть внутри группы томов можно создавать тома (аналог раздела на физическом жестком диске) и файловые системы внутри томов (рис. 1.14).

Необходимо заполнить следующие поля:

– имя тома – «var»;

– размер тома;

– разместить на следующих устройствах – «sda», «sdb».

Отметить «Создать том» и нажать «ОК».

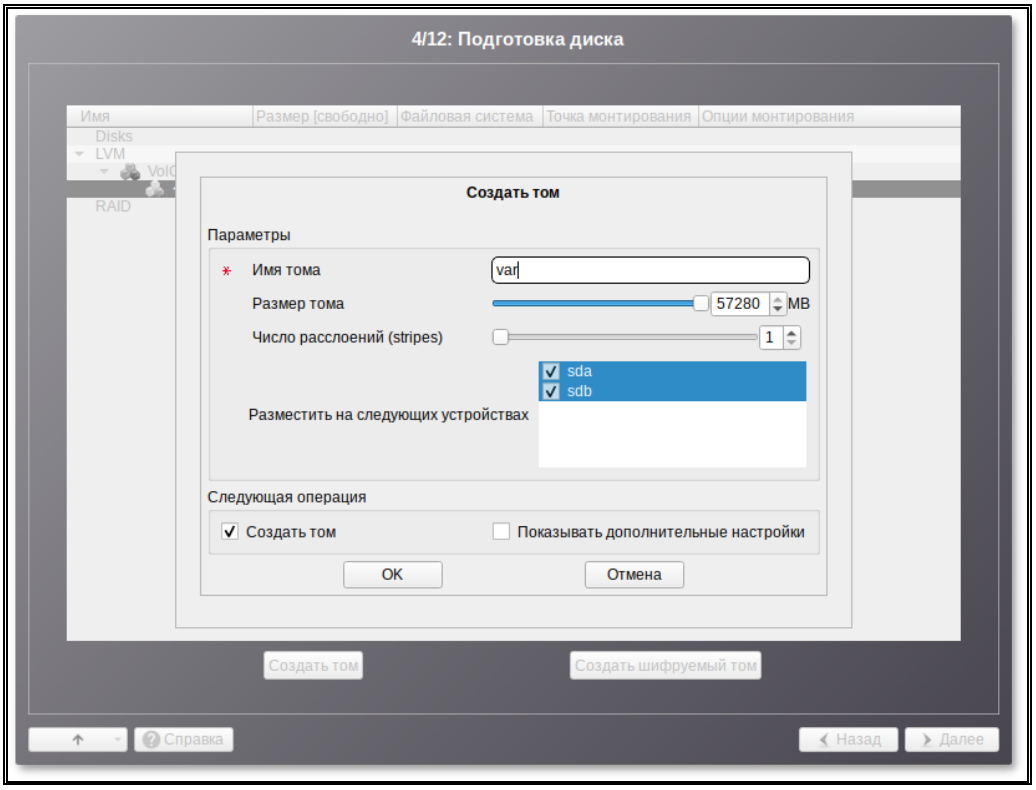

Рис. 1.14

7. Установка системы

7.1. На данном этапе происходит распаковка ядра и установка набора программ, необходимых для работы «Альт Сервер 10.1 для Эльбрус».

Программа установки предлагает выбрать дополнительные пакеты программ, которые будут включены в состав «Альт Сервер 10.1 для Эльбрус» и установлены вместе с ней на диск.

7.2. В процессе установки следует отказаться от установки дополнительных приложений (снять все «галочки»), оставить только «Systemd-networkd».

Под списком групп на экране отображается информация об объеме дискового пространства, которое будет занято после установки пакетов, входящих в выбранные группы (рис. 1.16).

Опция «Показать состав группы» выводит список программных пакетов, входящих в состав той или иной группы пакетов.

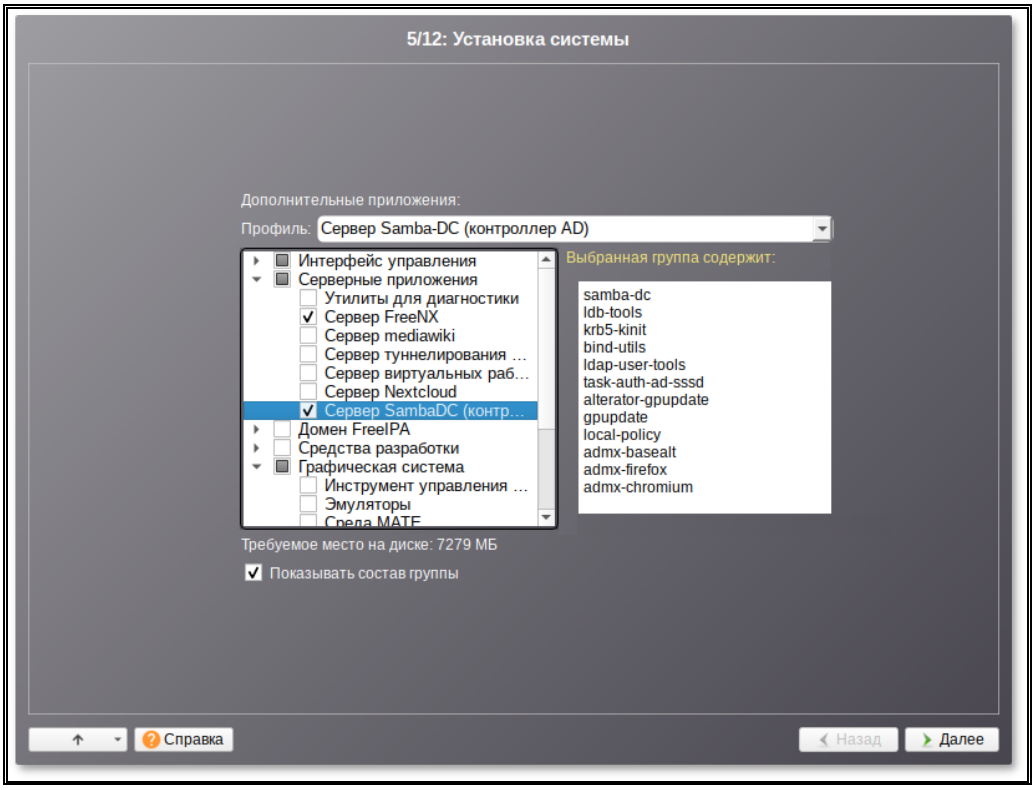

Рис. 1.15

Далее происходит установка набора программ, необходимых для работы системы (рис. 1.17).

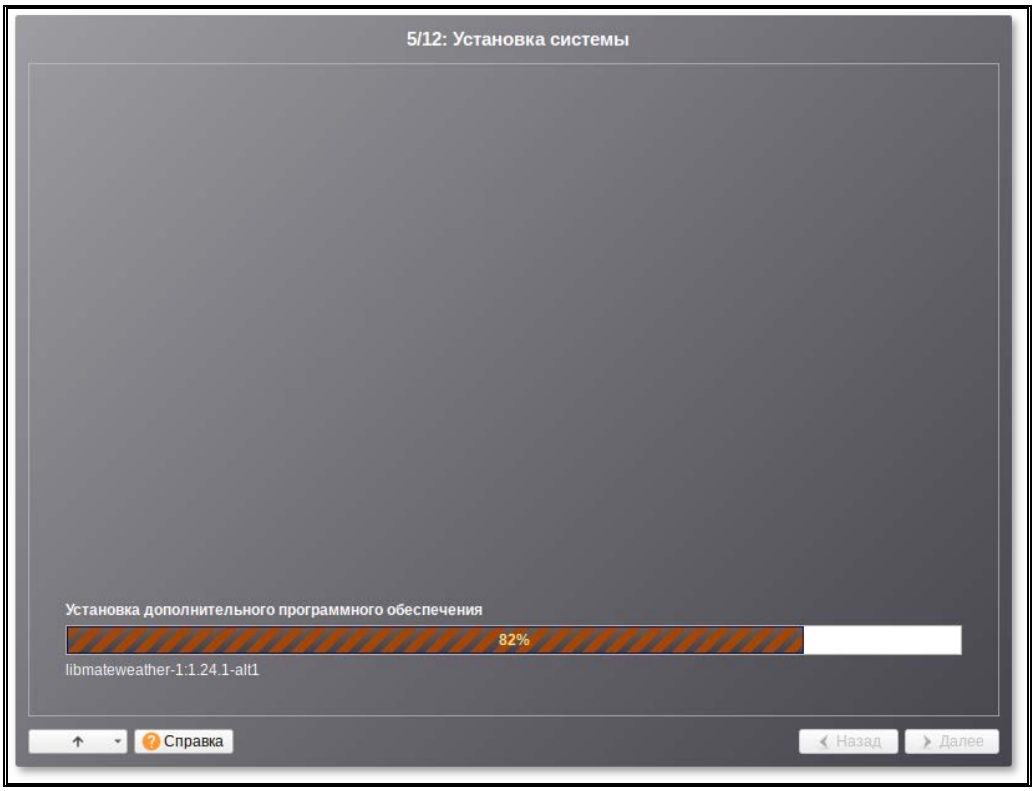

Рис. 1.16

8. Сохранение настроек

8.1. Начиная с данного этапа, программа установки работает с файлами только что установленной базовой системы. Все последующие изменения можно будет совершить после завершения установки посредством редактирования соответствующих конфигурационных файлов или при помощи модулей управления, включенных в дистрибутив.

8.2. По завершении установки базовой системы начинается шаг сохранения настроек. Он проходит автоматически и не требует вмешательства пользователя. На экране отображается индикатор выполнения.

Рис. 1.17

8.3. На этом шаге производится перенос настроек, выполненных на первых шагах установки, в только что установленную базовую систему. Также производится запись информации о соответствии разделов жесткого диска смонтированным на них файловым системам (заполняется конфигурационный файл «/etc/fstab»).

8.4. После сохранения настроек осуществляется автоматический переход к следующему шагу.

9. Настройка сети

9.1. На этом этапе необходимо задать параметры работы сетевой карты и настройки сети:

– IP-адреса сетевых интерфейсов;

– DNS-серверы,

– шлюз по умолчанию;

– домены поиска.

9.2. Конкретные значения будут зависеть от используемого пользователем сетевого окружения. Ручного введения настроек можно избежать при наличии в сети настроенного DHCP-сервера. В этом случае все необходимые сетевые настройки будут получены автоматически.

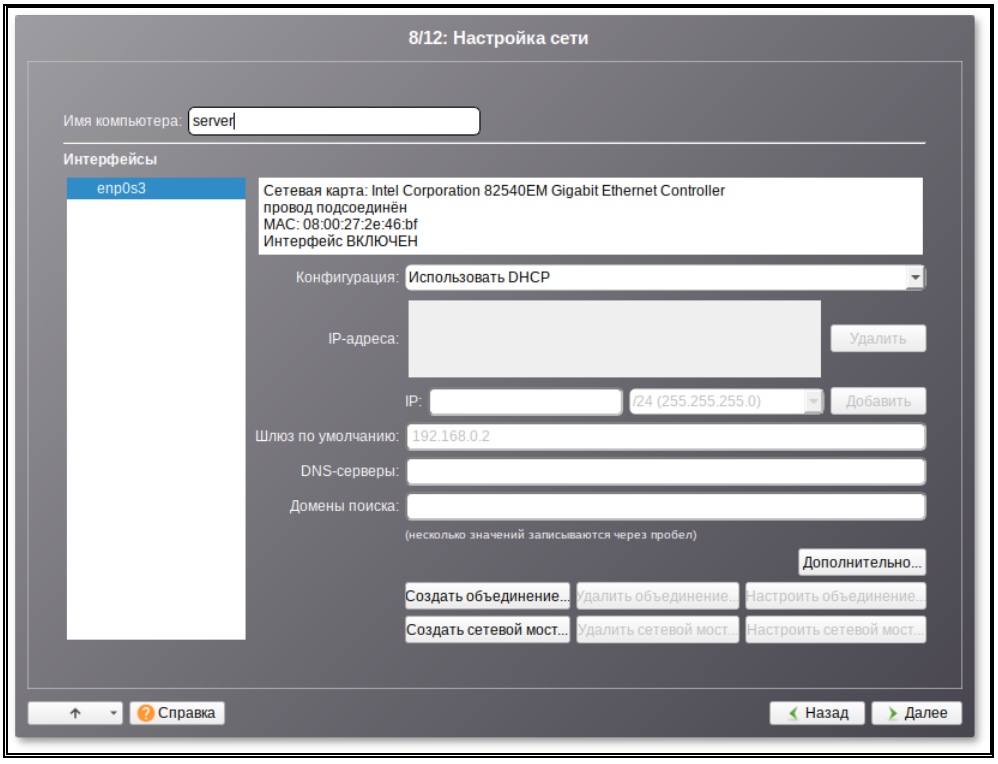

Рис. 1.18

9.3. Для сохранения настроек сети и продолжения работы программы установки необходимо нажать кнопку «Далее».

10. Администратор системы

10.1. На данном этапе загрузчик создает учетную запись администратора – «root». В открывшемся окне необходимо ввести пароль учетной записи администратора – «bazalt».

Чтобы исключить опечатки при вводе пароля, пароль учетной записи вводится дважды (рис. 1.20).

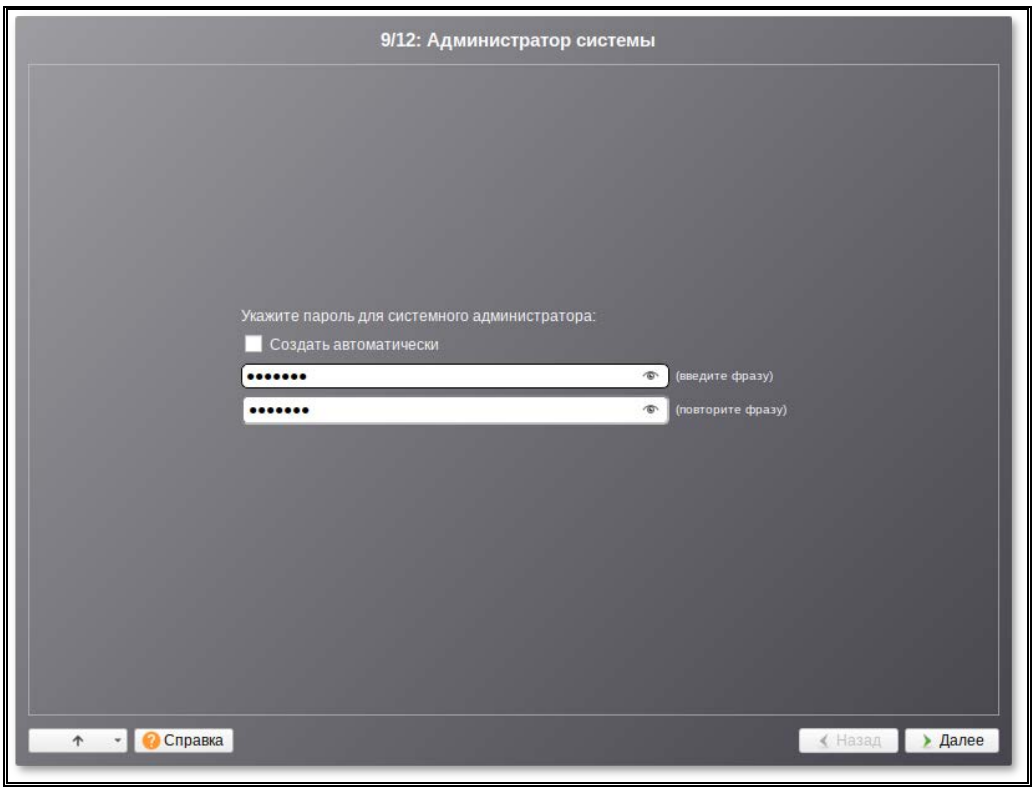

Рис. 1.19

11. Системный пользователь

11.1. На данном этапе программа установки создает учетную запись системного пользователя (пользователя) «Альт Сервер 10.1 для Эльбрус».

Необходимо ввести пользователя «altlinux» и пароль учетной записи пользователя – «bazalt» (рис. 1.21).

Для того чтобы исключить опечатки, пароль пользователя вводится дважды.

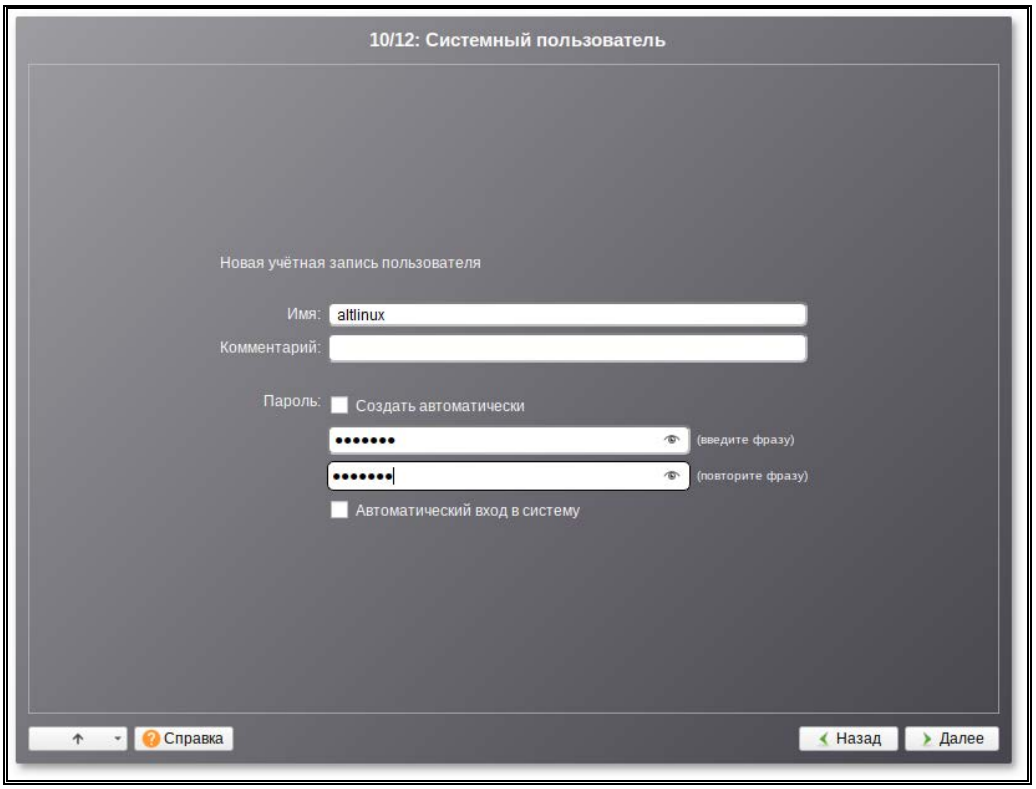

Рис. 1.20

12. Завершение установки

12.1. На экране последнего шага установки отображается информация о завершении установки «Альт Сервер 10.1 для Эльбрус».

После нажатия кнопки «Завершить» автоматически начнется перезагрузка системы.

12.2. Извлечь установочный DVD (если это не произошло автоматически). Теперь можно загружать установленную систему в обычном режиме.

ПРИЛОЖЕНИЕ 2

КОМАНДЫ CLI УПРАВЛЕНИЯ СПО ВП

1. В данном приложении приведено дерево команд СПО ВП. Фактически пользователь использует команды нижних уровней, но команды верхних уровней описаны, так как у них можно посмотреть «help».

2. Команды с пометкой «for support» необходимы в основном для команд технической поддержки и разработки, в связи с чем могут быть не полностью документированы.

3. Ниже приведены команды CLI для управления СПО ВП:

1) *help* – помощь по доступным в CLI командам;

2) *api* – команды работы в CLI с контроллером через REST API:

– *auth* – команда аутентификации в REST API контроллера СПО ВП;

– *datapool* – команды работы с пулами данных;

– *domain* – команды работы с ВМ;

– *node* – настройка узлов;

3) *backup* – команды управления резервными копиями настроек контроллера:

– *create* – создание резервной копии;

– *delete* – удаление ранее созданной копии;

– *list* – получение списка резервных копий;

– *restore* – восстановление из ранее созданной копии;

– *send* – копирование ранее созданной копии на другой сервер СПО ВП по SSH;

4) *cluster* – команды работы с кластером:

– *bootstrap_acl* – генерирует новый токен для консула;

– *config* – отображает конфигурацию кластера;

– *status* – отображает статус кластера;

5) *controller* – управление настройками, репликацией, базой данных контроллера:

– *add* – добавить контроллер для репликации;

– *backupdb_create* – создание резервной копии базы данных контроллера (в «/var/log/veil/controller/db_backup»);

– *backupdb_list* – проверка наличия резервной копии базы данных контроллера (из «/var/log/veil/controller/db_backup/main/backup_label»);

– *backupdb_restore* – восстановление базы данных контроллера (из «/var/log/veil/controller/db_backup»);

– *changepassword* – смена пароля базовой учетной записи «admin»;

– *check_remote_access* – проверка файлов редиректа «spice» для ВМ с таким же портом, удаление их и перезагрузка «nginx»;

– *clearsessions* – очистить сеансы базы данных («for support»);

– *collectstatic* – собрать статистику базы данных («for support»);

– *compilemessages* – компиляция сообщений базы данных («for support»);

– *db_check* – проверка целостности базы данных контроллера;

– *db_stats* – статистика базы данных контроллера

– *del* – удалить контроллер из репликации;

– *luns* – отображает LUNs в базе данных контроллера;

– *macs* – отображает имена и Mac-адреса всех интерфейсов в базе данных контроллера;

– *makemigrations* – миграция базы данных («for support»);

– *migrate* – применение новых миграций базы данных («for support»);

– *nginx_https* – перенаправление HTTP на HTTPS;

– *reload_node_streams* – переподключение сервиса контроллера к GRPC стримам узлов («for support»);

– *reload_queues* – делает запрос на переподключение к очередям («for support»);

– *repair_hosts* – проверка соответствия файла «hosts» таблице внутренних интерфейсов базы данных;

– *role* – смена роли контроллера;

– *showmigrations* – показать миграции базы данных («for support»);

– *status* – статус репликации;

6) *log* – команды вывода журналов:

– *audit* – чтение журналов аудита («/var/log/audit/audit.log*»);

– *auth* – чтение журналов авторизаций («/var/log/auth.log*»);

– *autotest* – чтение журналов системы автотестирования («/var/log/veil/puppet.log*»);

– *clear* – очистка файлов журналов;

– *cli* – чтение журналов CLI («/var/log/veil/cli/cli.log*»);

– *controller* – чтение журналов супервизора контроллера (controller-engine) («/var/log/veil/controller/controller.log*»);

– *controller_async* – чтение журналов асинхронных Web-сервисов контроллера (controller-web-proxy, controller-web-uploader) («/var/log/veil/controller/veil_async.log*»);

– *controller_web* – чтение журналов Web-интерфейса контроллера (controller-web-api) («/var/log/veil/controller/django.log*»);

– *controller_ws* – чтение журналов сервиса Web-сокетов контроллера (controller-websocket) («/var/log/veil/controller/websockify.log*»);

– *corosync* – чтение журналов сервиса «corosync» («/var/log/corosync/corosync.log*»);

– *first_boot* – чтение журналов скрипта послеустановочной инициализации («/var/log/veil/first_boot.log»);

– *first_tests* – вывод списка файлов автотестов после установки («for support»);

– *gluster* – чтение журналов сервиса «gluster» («/var/log/glusterfs/**/*.log»);

– *installer* – чтение журнала «syslog» установщика системы («/var/log/installer/syslog»);

– *kernel* – чтение журналов «kernel» («/var /log/kern.log*);

– *net_init* – чтение журналов скрипта установочной сетевой инициализации («/var/log/veil/auto_configure_nic.log»);

– *node* – чтение журналов супервизора узла (node-engine) («/var/log/veil/node/node.log*»);

– *node_async* – чтение журналов асинхронных Web-сервисов узла (node-web-proxy, node-web-uploader) («/var/log/veil/node/veil_async.log*»);

– *node_web* – чтение журналов Web-интерфейса узла (node-web-api) («/var/log/veil/node/django.log*»);

– *pgbouncer* – чтение журналов сервиса «pgbouncer» («/var/log/postgresql/pgbouncer.log*»);

– *postgresql* – чтение журналов сервиса «postgresql» («/var/log/postgresql/postgresql-11-main.log*»);

– *reboot* – чтение журналов перезагрузок и выключений узла;

– *redis* – чтение журналов сервиса «redis» («/var/log/redis/redis-server.log*»);

– *remove_archives* – рекурсивное удаление всех архивов журналов «.*gz*» из «/var/log/»;

– *rotate* – запуск ротирования журналов;

– *syslog* – чтение «syslog»;

7) *memory* – управление памятью:

– *cache_bench* – Explore the impact of virtual memory settings on caching efficiency on Linux systems under memory pressure;

– *drop_caches* – сброс кэша оперативной памяти. Запускайте команду, если вы точно понимаете, зачем она;

– *min_free_kbytes* – управление настройками «min_free_kbytes»;

– *nr_hugepages* – управление настройками «nr_hugepages»;

– *swappiness* – управление настройками «swappiness»;

– *vfscachepressure* – управление настройками «vfs_cache_pressure»;

8) *net* – настройка сетевой подсистемы узла:

– *conf* – команды конфигурации сетевой подсистемы узла:

а) *bonds* – команды конфигурации агрегированных интерфейсов сетевой подсистемы узла:

а1) *modify* – изменение агрегированного интерфейса;

а2) *remove* – удаление агрегированного интерфейса;

а) *debug* – управление «verbose» режимом сервиса «networking»;

б) *dns* – команды конфигурации «dns» сетевой подсистемы узла:

в1) *flush* – сброс настроек DNS*;*

в2) *set-dhcp* – настройка DNS dhcp*;*

в3) *set-static* – настройка статики DNS*;*

в) *ip* – команды конфигурации адресации сетевой подсистемы узла:

г1) *renew-lease* – запрос продления аренды адреса интерфейса управления;

г2) *set-dhcp* – задание динамического адреса интерфейса управления;

г3) *set-static* – задание статического адреса интерфейса управления;

г) *ports* – команды конфигурации портов сетевой подсистемы узла:

д1) *blink* – «моргание» физических интерфейсов;

д2) *release* – сброс настройки сетевых портов;

д3) *set-default-bond* – установка агрегированного интерфейса;

д4) *set-default-port* – установка базового физического интерфейса;

д5) *set-down* – отключение порта;

д6) *set-mtu* – установка «mtu» физического интерфейса;

д7) *set-promisc* – управление неразборчивым режимом портов;

д8) *set-up* – включение физического порта;

д) *routing* – команды конфигурации маршрутизации сетевой подсистемы узла:

е1) *add-static* – добавляет маршрут;

е2) *default* – настройка базового маршрута;

е3) *del-static* – удаление маршрута;

е4) *flush* – сброс таблицы маршрутизации;

е) *vlan* – команды конфигурации «vlan» сетевой подсистемы узла:

ж1) *flush* – сброс VLAN интерфейса управления;

ж2) *set* – настройка VLAN интерфейса управления;

ж) *vswitches* – управление виртуальными коммутаторами:

з1) *flush* – сброс настроек виртуального коммутатора;

– *firewall* – управление сервисом межсетевого экрана;

– *flush* – сброс существующей сетевой конфигурации;

– *info* – выводит общую информацию о текущих настройках сети управления;

– *init* – ручная инициализация сети узла;

– *lldp* – команды управление сервисом LLDP;

– *mtu-finder* – поиск оптимального MTU для интерфейса;

– *show* – вывод информации о текущих настройках сетевой подсистемы:

з) *bonds* – информация по агрегированным интерфейсам;

и) *dns* – информация по настройкам DNS;

к) *ip* – информация по настройкам IP-адреса интерфейса управления;

л) *lldp* – информация о демоне LLDP;

м) *ports* – информация о сетевых портах;

н) *routing* – информация по настройкам маршрутизации;

о) *vlan* – информация по настройкам VLAN интерфейса управления;

п) *vnetworks* – информация о конфигурации существующих виртуальных сетей;

р) *vswitches* – информация о виртуальных коммутаторах;

9) *node* – команды работы с узлами:

– *cli* – подключение к узлу и запуск команды cli;

– *collectstatic* – сбор статистики данных узла («for support»);

– *config* – отображает конфигурацию узла;

– *controller_ip* – отображает адрес контроллера;

– *controller_status* – отображает статус связи с контроллером;

– *copy* – копирование файлов с контроллера через SSH на все узлы;

– *id* – отображает UUID узла;

– *list* – отображает список узлов;

– *makemigrations* – миграция базы данных узла («for support»);

– *migrate* – применение миграции базы данных узла («for support»);

– *multipath_sync* – синхронизация файла конфигурации «multipath» между контроллером и узлами;

– *nodes_cli* – подключение ко всем узлам и запуск команды CLI;

– *reload_queues* – делает запрос на переподключение к очередям контроллера («for support»);

– *repo_sync* – синхронизация репозиториев между контроллером и узлами;

– *restart_supervisors* – перезапуск супервизоров всех узлов (node-engine);

– *set_hostname* – установка «hostname» узла;

– *showmigrations* – показать миграцию базы данных узла («for support»);

– *ssh* – подключение через SSH к узлу;

– *status* – операции со статусом узла;

– *sync* – синхронизация node and cli env and app между контроллером и узлами («for support»);

– *task* – задачи узла (активные и в кэше);

– *upgrade_start* – подключение к узлу и запуск команды «upgrade start»;

– *web* – node web commands;

10) *services* – сервисы системы управления:

– *cat* – просмотр сервисов системы управления;

– *list* – список и статус сервисов системы управления;

– *restart* – перезапуск сервисов системы управления;

– *start* – запуск сервисов системы управления;

– *stop* – останов сервисов системы управления;

11) *ssh* – управление доступом по SSH:

– *disable* – ограничивает возможность новых подключений к узлу по SSH. Текущие SSH сессии продолжат работу, но при переподключении доступ будет ограничен;

– *enable* – включает доступ к узлу по SSH для всех разблокированных пользователей;

– *session* – управление сессиями по SSH:

с) *client_alive_count_max* – команда просмотра и изменения количества периодов до отключения неактивного пользователя. Для изменения параметра ввести значение в диапазоне от «0» до «10». Для просмотра текущего значения выполнить без значения;

т) *client_alive_interval* – команда просмотра и изменения количества времени (секунды), по истечению которого неактивный пользователь будет отключен. Для изменения параметра ввести значение в диапазоне от «0» до «7200». Для просмотра текущего значения выполнить без значения;

у) *list* – вывод активных сессий;

ф) *maxauthtries* – команда просмотра и изменения количества неудачных попыток подключения. Для изменения параметра ввести значение в диапазоне от «0» до «10». Для просмотра текущего значения выполнить без значения;

х) *maxlogins* – команда просмотра и изменения количества одновременных подключений каждого пользователя. Для изменения параметра ввести значение в диапазоне от «1» до «10». Для просмотра текущего значения выполнить без значения;

ц) *maxsessions* – команда просмотра и изменения количества мультиплексированных сеансов SSH в течение одного сеанса SSH. Для изменения параметра ввести значение в диапазоне от «1» до «30». Для просмотра текущего значения выполнить без значения;

ч) *maxsyslogins* – команда просмотра и изменения общего количества одновременных подключений. Для изменения параметра ввести значение в диапазоне от «1» до «30». Для просмотра текущего значения выполнить без значения;

– *status* – отображает статус SSH доступа на узле;

– *user* – управление SSH пользователями:

ш) *add* – добавляет пользователя в операционную систему узла, которому может быть открыт SSH доступ;

щ) *change_password* – изменяет пароль SSH пользователя узла;

ы) *list* – отображает список пользователей SSH системы узла. Заблокированный пользователь будет иметь соответствующую метку;

э) *lock* – блокирование пользователей SSH на узле. Заблокированные подключенные пользователи смогут продолжить работу, но при переподключении доступ будет ограничен;

ю) *remove* – удаляет SSH пользователя из системы узла;

я) *unlock* – разблокирование пользователей SSH на узле;

12) *storage* – команды для работы с хранилищами:

– *clear_iscsiadm_base* – удаление активных iSCSI подключений («for support»);

– *corosync_conf* – вывод файла конфигурации «corosync» («for support»);

– *discovery* – сканирование доступных FC и iSCSI блочных хранилищ;

– *dlm_conf* – вывод файла конфигурации «dlm» («for support»);

– *fc_luns* – вывод доступных FC LUNs;

– *fc_wwns* – вывод доступных WWN FC хранилищ;

– *fio_test* – тест через FIO;

– *fstab* – вывод fstab («/etc/fstab»);

– *gfs2* – вывод статуса кластерного хранилища «gfs2» (corosync, dlm, mountpoints);

– *gluster* – вывод статуса «gluster»;

– *hba_npiv* – вывод доступных HBA (NPIV subsystem);

– *initiator_name* – вывод InitiatorName;

– *iscsi_configs* – вывод доступных iSCSI configs («for support»);

– *iscsi_luns* – вывод доступных iSCSI LUNs;

– *local_wwns* – вывод локальных FC WWN;

– *luns* – вывод всех доступных FC and iSCSI LUNs;

– *modify_initiator_name* – изменение InitiatorName;

– *modify_multipath_path_grouping_policy* – изменение «multipath path_grouping_policy»;

– *modify_multipath_path_selector* – изменение «multipath path_selector»;

– *multipath* – вывод полной конфигурации «multipath»;

– *multipath_conf* – вывод файла конфигурации «multipath»;

– *multipath_conf_set_default* – сброс файла конфигурации «multipath» до базового;

– *multipath_edit* – изменение файла конфигурации «multipath»;

– *ocfs2* – вывод статуса «ocfs2»;

– *pool_create* – создания пула (NPIV subsystem);

– *pool_destroy* – удаление пула (NPIV subsystem);

– *pools* – вывод доступных пулов (NPIV subsystem);

– *remove_fstab* – удаление записи из «fstab» («for support»);

– *rescan_scsi_bus* – сканирование шины SCSI;

– *rescan_vhba* – сканирование NPIV LUNs (NPIV subsystem);

– *scsi_host_discovery* – сканирование SCSI hosts;

– *vols* – вывод доступных «vols» (NPIV subsystem);

– *zfs* – сканирование «zfs»;

13) *system* – управление системными ресурсами:

– *autotest* – автотестирование системы;

– *cmdline* – команда просмотра и модификации параметров загрузки ядра Linux;

– *dmidecode* – вывод DMI записей из SMBIOS;

– *dynmotd* – динамическое сообщение дня «dynmotd»;

– *hypervisor_size* – вывод размера гипервизора;

– *info* – информация о базовой системе сервера;

– *init* – start system init («for support»);

– *kaspersky* – команды работы с Kaspersky Endpoint Security;

– *language* – команды просмотра и установки системного языка CLI;

– *license* – вывод информации о текущем лицензионном ключе;

– *logging* – информация о состоянии БД событий;

– *nested* – управление вложенной виртуализацией;

– *pci* – управление настройками IOMMU;

– *repo* – управление источниками приложений;

– *statistics* – информация о сборе статистики серверов;

– *vulnerability* – проверка уязвимостей процессора системы;

– *watchdog* – команды работы с «watchdog»;

14) *upgrade* – обновление ПО СПО ВП:

– *aptautoremove* – автоматическое удаление ненужных пакетов;

– *cache* – проверяет наличие обновлений в «apt cache»;

– *check* – проверка наличия обновлений;

– *download* – загружает обновления в «apt cache»;

– *local* – используется, если у СПО ВП нет возможности получить доступ к источнику обновлений. Используется механизм «apt-offline»:

аа) *prepare* – подготовка к offline-обновлению. Запись на USB текущего состояния пакетов;

бб) *proceed* – устанавливает или обновляет пакеты с apt-offline ZIP;

– *log* – просмотр результатов установки обновлений;

– *proxy* – управление обновлением узлов через контроллер;

– *release* – установка релизного обновлений;

– *removelock* – удаление файла блокировки обновления;

– *start* – установка обновлений;

15) *vm* – команды управления виртуальными машинами:

– *capabilities* – вывод возможностей гипервизора;

– *console* – подключение к консоли ВМ;

– *full_list* – вывод списка ВМ на всех узлах (с контроллера);

– *guest_ad* – информация о вхождении ВМ в AD;

– *guest_add_to_ad* – добавление ВМ в AD;

– *guest_fs_info* – информация о файловой системе ВМ;

– *guest_get_devices* – информация о устройствах ВМ;

– *guest_get_disks* – информация о дисках ВМ;

– *guest_info* – информация о гостевом агенте ВМ;

– *guest_rm_from_ad* – удаление ВМ из AD;

– *hostname* – hostname ВМ;

– *interfaces* – сетевые интерфейсы ВМ;

– *list* – вывод списка ВМ;

– *log* – журналы ВМ;

– *memory_params* – статистика памяти ВМ;

– *memory_stats* – статистика памяти ВМ;

– *metadata* – metadata ВМ;

– *reboot* – перезагрузка работы ВМ;

– *reset* – принудительная перезагрузка работы ВМ;

– *resume* – продолжение работы ВМ;

– *schedinfo* – информация планировщика процессора ВМ;

– shutdown – выключение ВМ;

– *start* – запуск ВМ;

– *suspend* – приостановка ВМ;

– *xml* – xml ВМ;

16) *aide* – система обнаружения проникновения;

17) *backup-os* – команда создания резервных копий операционной системы сервера;

18) *boot_protect* – команды управления парольной защитой загрузчика узла;

19) *cmd* – команды узла («for support»);

20) *dumphelp* – автогенерация документации по командам CLI («for support»);

21) *elasticsearch* – команды останова и запуска Elasticsearch;

22) *grafana* – команды останова и запуска Grafana;

23) *hosts* – команда вывода файла «/etc/hosts»;

24) *install* – устанавливает пакеты из репозитория;

25) *install-deb* – устанавливает deb-пакеты с USB-накопителя;

26) *install-rpm* – устанавливает rpm-пакеты с USB-накопителя;

27) *install-run* – запускает «.run» файлы из датапулов, имеющихся на узле;

28) *ipmi* – получает текущий IPMI IP;

29) *kibana* – команды останова и запуска «kibana»;

30) *limits* – системные ограничения процессора и памяти;

31) *ntp* – команды работы с NTP;

32) *nvidia* – команды управления Nvidia GRID;

33) *poweroff* – выключение узла;

34) *rdma* – команды для работы с «rdma»;

35) *reboot* – перезагрузка узла;

36) *stats* – статистика очередей «beanstalk»;

37) *status* – просмотр последнего состояния сбора информации супервизора узла;

38) *upload_file* – команды загрузки файлов в локальный пул данных;

39) *upload_iso* – команды загрузки образов в локальный пул данных;

40) *upload_guest_utils* – команды загрузки «guest_agent» в локальный пул данных.

41) *version* – возвращает информацию о версиях установленного ПО СПО ВП;

42) *vsftpd* – команды останова и запуска «vsftpd»;

43) *wipefs* – команда удаляет файловые системы с выбранных накопителей. При вызове без параметров отображается интерактивный браузер для выбора дисков.

Перечень принятых сокращений

АРМ	– автоматизированное рабочее место
БД	– база данных
ВМ	– виртуальная машина
ВУ	– вычислительный узел
МК	– менеджер конфигурации
НЖМД	– накопитель на жестком магнитном диске
ОС	– операционная система
ПО	– программное обеспечение
ЭВМ	– электронно-вычислительная машина
AD	– Active Directory (активный каталог)
API	– Application Programming Interface (интерфейс программирования приложений)
CLI	– Command Line Interface (интерфейс командной строки)
IPMI	– Intelligent Platform Management Interface (интеллектуальный интерфейс управления платформой)
LDAP	– Lightweight Directory Access Protocol (облегченный протокол доступа к каталогам)
LVM	– Logical Volume Manager (менеджер логических томов)
PXE	– Preboot Execution Environment (среда для загрузки компьютера с помощью сетевой карты без использования локальных носителей данных)
SSO	– Single Sign-On (технология единого входа)

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	Номер документа	Входящий номер сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					