Astra
Infrastructure
Cloud

Руководство администратора облачной платформы базовой конфигурации Astra Infrastructure Cloud (AIC)

Оглавление

Введение

Настоящий документ является руководством администратора программного изделия «Облачная платформа «Astra Infrastructure Cloud». (далее — AIC) и предназначен для администраторов операционной системы специального назначения «Astra Linux Special Edition», осуществляющих установку и развертывание Облачной платформы.

В документе приведено описание порядка развертывания и настройки AIC с учетом особенностей ALSE и других компонентов платформы, под управлением которых функционирует AIC.

Облачная платформа (ОП) «AIC» предназначена для установки в ЦОД Заказчика и основана на базе ПО Группы Астра.

Базовые компоненты:

- Операционная Система Специального Назначения «Astra Linux SE»;
- программный комплекс средств виртуализации «Брест»;
- программный комплекс для централизованного администрирования и службы каталогов «ALD Pro»;
- система резервного копирования «RuBackup».

Дополнительные компоненты, список которых может варьироваться при необходимости:

- ПО для автоматизации развертывания приложений «Astra Automation»;
- ПО для мониторинга компонентов платформы «Astra Monitoring»;
- ПО для управления физической ИТ-инфраструктурой «DCImanager»;

ПО для биллинга и автоматизации предоставления ресурсов «BILLmanager»

Ключевые понятия

Архитектурная концепция для комплексного решения «AIC» представляет собой многокомпонентное модульное решение, обеспечивающее полную функциональность “облака из коробки” ("out-of-the-box"), которое может быть реализовано в конфигурациях с минимальным набором или несколькими узлами как на площадке в выделенном ЦОД, так и на стороне Заказчика.

1. Архитектурная концепция:

   Архитектурная концепция для комплексного решения AIC определяет основные принципы и структуру решения, которое позволяет обеспечить масштабируемость, надежность и безопасность для различных рабочих нагрузок и требований клиентов.

2. Многокомпонентное модульное решение:

   AIC состоит из нескольких отдельных компонентов, которые могут быть легко интегрированы и настроены для обеспечения полной функциональности "облака из коробки".

3. Функциональность "облака из коробки" ("out-of-the-box"):

   означает, что AIC предоставляет полный набор инструментов и возможностей для быстрой и эффективной реализации облачных решений без необходимости дополнительной интеграции и настройки.

4. Конфигурации с минимальным набором или несколькими узлами:

   AIC может быть реализован как на площадке в выделенном ЦОД, так и на стороне Заказчика. Это позволяет клиентам выбирать оптимальную конфигурацию в зависимости от своих потребностей и ресурсов.

Базовая редакция облачной платформы

Архитектура облачной платформы AIC представляет собой модульное масштабируемое решение, обеспечивающее необходимую функциональность управления облачными вычислительными ресурсами.

Облачная платформа включает в себя следующий набор продуктов группы компаний Астра:

С точки зрения общей архитектуры, облако представляет собой единый взаимосвязанный набор программных и инфраструктурных блоков, каждый из которых может независимо масштабироваться, предоставляя возможность гибко изменять:

- вычислительные ресурсы (конфигурацию серверов);
- системы хранения данных (объемы и распределение хранилищ данных);
- сетевые ресурсы (коммутаторы, маршрутизаторы, межсетевые экраны).

Базовая редакция включает минимально необходимый набор компонентов, позволяющий использовать основные возможности ОП с дальнейшим расширением функционала за счёт добавления необходимых компонент Стандартной Редакции или собственных разработок.

Компоненты Базовой Редакции:

- ОС СН «Astra Linux SE»;

- ПК СВ «Брест»;
- ПК службы каталогов «ALD Pro»;
- СРК «RuBackup»;
- ПО «DCImanager» (опционально - с ограничениями);
- ПО «Astra Monitoring» (опционально - с ограничениями).

ОС СН Astra Linux - операционная система, являющаяся основой для построения ОП AIC

ПК СВ «Брест» предназначен для создания виртуальной среды, обеспечивающей функционирование виртуальных машин и управление ими, в операционной системе специального назначения «Astra Linux Special Edition». Облачные сервисы ПК СВ "Брест" имеют встроенный механизм обеспечения отказоустойчивости высокой доступности. Для его задействования разворачивается нечетное количество экземпляров Front-end, которые взаимодействуя между собой по алгоритму RAFT, обеспечивают доступность сервисов управления облаком при отказе менее половины узлов.

Узлы, взаимодействуя по алгоритму RAFT, определяют лидера, который обслуживает все входящие запросы, для чего выделяется "плавающий" (переходящий от узла к узлу) IP-адрес. Каждый узел имеет свой экземпляр БД, который реплицируется сервисами, обслуживающими облако.

ALD Pro – программный комплекс для централизованного управления доменом на базе ОС Astra Linux.

ALD Pro представляет собой набор интегрированных между собой модулей, составляющих полноценный инструмент для администрирования учётных записей пользователей и подразделений, ПК и серверов. В ALD Pro реализованы механизмы для управления групповыми политиками, детальной настройки домена, мониторинга ресурсов контроллера домена и аудита событий. Предоставляет возможность выстраивать иерархии подразделений и назначать им групповые политики.

RuBackup – система резервного копирования и восстановления данных.

BILLmanager - оркестратор, позволяет управлять доступом, квотами, объёмами ресурсов, включением-выключением виртуальных машин, их конфигурацией, предоставляет возможность формирования отчётов и статистики использования вычислительных ресурсов.

DCImanager — платформа централизованного управления оборудованием: стойками, серверами, сетевым оборудованием, PDU, ИБП, физическими и

виртуальными сетями. DCImanager работает с мультивендорным парком отечественных и зарубежных серверов, отслеживает их состояние и прогнозирует отказы компонентов на физическом уровне, без использования агентов. DCImanager регистрирует действия пользователей, управляет питанием, позволяет автоматически устанавливать ОС и ПО.

Astra Monitoring — программная платформа для мониторинга продуктов ГК Астра, а также физической, виртуальной инфраструктуры, сервисов, приложений, сбора и анализа журналов событий, оповещений (alerts), и построения базовых отчётов о состоянии инфраструктуры. В составе облачной платформы обеспечивает: мониторинг состояния компонентов платформы, централизованный сбор событий и системных журналов.

Astra Automation — программный комплекс для автоматизированного и безопасного развёртывания ПО серверной ИТ-инфраструктуры на базе продуктов ГК Астра и других производителей, а также управления конфигурациями. В составе облачной платформы обеспечивает: автоматизацию развёртывания компонентов платформы, а также сложных сценариев развёртывания сервисов (SaaS/PaaS)

Требования к среде функционирования

Базовый компонент AIC - ПК СВ «Брест» функционирует только под управлением ОС СН на максимальном уровне защищенности («Смоленск») или усиленном уровне защищенности («Воронеж»).

Для обеспечения корректного функционирования ПК СВ необходимо установить программное обеспечение оперативных обновлений ОС СН бюллетень № 2023-0426SE17 (оперативное обновление 1.7.4) и бюллетень № 2023-0630SE17MD (оперативное обновление 1.7.4.UU.1).

После установки оперативного обновления рекомендуется применение ядра linux-5.15-generic.

Требования к техническим средствам

ПК СВ функционирует в следующем режиме:

- в дискреционном режиме обеспечивается функционирование защищенной среды виртуализации, в том числе дискреционное и мандатное управление доступом к ВМ. В таком режиме ВМ запускаются от имени доменного

пользователя, авторизовавшегося в ПК СВ. Для работы в дискреционном режиме необходимо, чтобы все компьютеры, на которых развернуты программные компоненты ПК СВ, входили в один домен ALD Pro.

Режим функционирования устанавливается на этапе развертывания ПК СВ. После установки и инициализации программных компонент переключение режимов функционирования ПК СВ не предусмотрено.

Создание и защита среды виртуализации обеспечиваются встроенными средствами ОС СН, интегрированными с подсистемой безопасности PARSEC, предназначенной для реализации функций ОС СН по защите информации от несанкционированного доступа:

- модулем ядра KVM, который использует аппаратные возможности архитектуры x86-64 по виртуализации процессоров;
- средствами эмуляции аппаратного обеспечения на основе QEMU;
- сервером виртуализации на основе libvirt.

В ПК СВ входят следующие программные компоненты серверной части:

- сервер виртуализации — для возможности создания виртуальных машин посредством эмуляции аппаратного обеспечения;
- сервер управления — для возможности управления через веб-интерфейс, из командной строки (консольный интерфейс) и с помощью XML-RPC API.

В качестве клиентской части изделия может выступать средство вычислительной техники, с которого выполняется подключение к серверу управления или виртуальной машине (ВМ).

В качестве дополнительных программных компонентов (не входят в состав ПК СВ) выступают:

- хранилище — система, предназначенная для хранения образов дисков виртуальных машин. Может быть построена на базе следующих технологий хранения:
  - файловой технологии хранения
  - блочной технологии хранения с использованием LVM;
  - программно-определяемой технологии хранения Ceph;
- контроллер домена — служба, обеспечивающая аутентификацию пользователей в рамках единого пространства пользователей (не используется в сервисном режиме работы ПК СВ).

П р и м е ч а н и е. В ПК СВ в качестве службы управления единым пространством пользователей используется ALD Pro из состава ОС СН. Если на объекте

эксплуатации уже имеется настроенный домен ALD Pro, то разворачивать дополнительный контроллер домена нет необходимости. Все серверы вводятся в существующий домен.

ПК СВ может быть развернут как на группе компьютеров, так и на виртуальных машинах в пределах одного компьютера для тестирования. Для объединения компьютеров, обеспечения выполнения операций управления и поддержки виртуальных сетей используется локальная сеть.

ВНИМАНИЕ! Программные компоненты ПК СВ должны функционировать на оборудовании, отвечающему требованиям к аппаратному обеспечению под управлением ОС СН.

П р и м е ч а н и е. Если для установки сервисов ПК СВ планируется использовать оптические установочные носители, то серверы должны быть оборудованы устройством для чтения и записи CD и DVD.

- Требования сервера управления:

Минимальные рекомендуемые характеристики компьютера для развертывания службы сервера управления указаны в таблице ниже:

Ресурсы	Минимальная рекомендуемая конфигурация
Память	4ГБ
ЦП	1 ЦП (2-ядра)
Размер диска	100 ГБ
Сеть	2 NICS

Максимальное количество серверов виртуализации (компьютеров, на которых установлена и инициализирована служба сервера виртуализации), которым можно управлять с помощью одного экземпляра сервера управления, зависит от производительности и масштабируемости инфраструктуры ПК СВ и главным образом от системы хранения данных.

Не рекомендуется использовать один экземпляр сервера управления для управления более чем 500 серверами виртуализации.

Сервер управления (компьютер, на котором установлена и инициализирована служба сервера управления) должен иметь сетевое соединение со всеми серверами виртуализации и, по возможности, доступ к хранилищам данных (как локальным, так и сетевым). Для обеспечения надежности инфраструктуры ПК СВ рекомендуется использовать как минимум две сети (соответственно, требуется два сетевых интерфейса):

1) сервисная сеть — используется службой сервера управления для обеспечения доступа к серверам виртуализации с целью управления и мониторинга гипервизоров и перемещения файлов образов;
2) сеть экземпляров — обеспечивает возможность сетевого подключения к виртуальным машинам через различные серверы виртуализации.

Кроме того, может потребоваться третий сетевой интерфейс для обеспечения доступа к сети хранения данных.

- Требования сервера виртуализации:

Минимальные рекомендуемые характеристики компьютера для развертывания службы сервера виртуализации:

1) процессорная архитектура x86-64 с аппаратной поддержкой виртуализации (Intel VT, AMD-V);

2) центральный процессор (ЦП) — без последующих дополнительных нагрузок каждый модуль ЦП, закрепленный за одной ВМ, должен соответствовать физическому ядру ЦП в случае, если необходимо минимизировать конкуренцию ВМ за процессорные ядра. Например, при нагрузке в 40 виртуальных машин с двумя ЦП каждая, потребуются 80 физических ЦП. При этом 80 физических ЦП могут распределяться по различным серверам виртуализации: 10 компьютеров с восемью ядрами каждый или пять компьютеров с 16 ядрами каждый. При необходимости последующих дополнительных нагрузок архитектуру ЦП можно планировать заранее с помощью элементов CPU и VCPU: CPU определяет физические ЦП, закрепленные за виртуальными машинами, а VCPU — виртуальные ЦП, передаваемые гостевой операционной системой;

3) оперативная память — по умолчанию в ПК СВ отсутствует избыточно выделяемая память. Как правило, рекомендуется всегда предусматривать резерв 10 % по ресурсам, потребляемым гипервизором. Например, для нагрузки в 40 виртуальных машин с 2 ГБ оперативной памяти каждая необходимо около 90 ГБ физической памяти (с учетом ресурса оперативной памяти, потребляемый гипервизором). Например, пять компьютеров с 24 ГБ оперативной памяти каждый предоставят по 22 ГБ памяти, поэтому они смогут выдержать планируемую нагрузку;

4) объем свободного системного дискового пространства — не менее 30 ГБ.

В каждом сервере виртуализации в зависимости от конфигурации хранилища и сети должно быть установлено до четырех сетевых интерфейсов: для сети экземпляров (приватной и/или публичной), сервисной сети и сети хранения данных.

Ролевая модель

Типы пользователей AIC

В облачной платформе AIC существуют следующие типы пользователей:

- Супер администраторплатформы
- Администратор тенанта/ выделенного пула ресурсов
- Пользователь тенанта
- Бизнес пользователь тенанта
- Аудитор
- Офицер безопасности облака
- Офицер безопасности тенанта

Типы пользователей ПК СВ Брест

Пользователь в ПК СВ определяется по имени и паролю. Создавать новую учетною запись в ОС СН для каждого пользователя ПК СВ не требуется. Аутентификация пользователей ПК СВ осуществляется при помощи строки сессии в каждой операции, которая проверяется ядром ПК СВ (службой oned). Каждый пользователь обладает уникальным идентификатором и принадлежит к группе.

При первом запуске ПК СВ автоматически создаются следующие группы:

- brestadmins — администраторы ПК СВ, обладают полномочиями, чтобы выполнить любую операцию в отношении любого объекта. При этом в этой группе автоматически создаются следующие пользователи:
  - oneadmin — используется для взаимодействия всех систем ПК СВ,
  - serveradmin — используется сервисом веб-интерфейса ПК СВ для взаимодействия с другими сервисами ПК СВ;
- brestusers — пользователи инфраструктуры, имеют доступ к большей части функционала, предлагаемого ПК СВ для управления ресурсами.

Кроме того, при инициализации сервиса фронтальной машины в ПК СВ создается пользователь группы администраторов ПК СВ:

- в сервисном режиме функционирования ПК СВ — пользователь brestadmin;
- в дискреционном режиме функционирования ПК СВ — доменный пользователь, имя которого указывается вручную при инициализации сервиса фронтальной машины.

На основе VDC созданы три базовые группы пользователей:

- *org_user* может просматривать список созданных виртуальных машин в рамках тенанта и может подключаться по VNC.
- *org_poweruser* может создавать виртуальные машины, шаблоны виртуальных машин, образы и сети (images, vm, vm templates, networks на основании vn templates).

- *org_admin* может создавать шаблоны виртуальных машин, группы безопасности (vm templates, security groups) и адмистрировать группы тенанта: добавлять пользователей платформы в группы тенанта.

Тенантом являются ресурсы, созданные внутри этих 3-х групп и ресурсы, доступные с VDC. Группы имеют различные права в рамках тенанта.

Диаграмма, описывающая ролевую модель доступа к облачным ресурсам приведена в Приложении Д (Рисунок 27).

Порядок управления пользователями в ПК СВ представлен в документе «Программный комплекс «Средства виртуализации «Брест» (ПК СВ «Брест») РДЦП.10001-02. Руководство администратора. Часть 2»

Типы пользователей RuBackup

В СРК RuBackup реализована ролевая модель доступа, т. е. назначение типа пользователя и предоставление ему набора полномочий для выполнения определенных рабочих задач в соответствии с его ролью.

В СРК RuBackup предусмотрены следующие типы пользователей:

- Администратор
- Мейтенер
- Суперпользователь
- Пользователь RuBackup

Суперпользователь RuBackup является привилегированным администратором, которому позволены любые действия в СРК. Суперпользователь и база данных создаются по умолчанию как rubackup, однако в дальнейшем их можно переименовать по своему усмотрению. Суперпользователь rubackup создается при создании базы данных rubackup и является владельцем базы данных. Таким образом, в списке пользователей СРК пользователя rubackup нельзя увидеть и нельзя создать еще одного пользователя rubackup.

Суперпользователь rubackup имеет следующие возможности:

- добавлять новых пользователей в систему. При этом выбранная группа пользователя влияет только на задачи уведомления. Чтобы пользователь мог получить административные привилегии в СРК, его нужно добавить в суперпользователи, мейнтейнеры или администраторы;
- менять пароль для других пользователей с помощью RuBackup Management

Супервайзер может выполнять любые действия, кроме добавления новых пользователей в СРК и кроме изменения глобальных настроек СРК.

Сопровождающий отвечает за медиасервер и может управлять устройствами хранения на этом медиасервере.

Администратор отвечает за группу клиентов и может выполнять их настройки и действия, связанные с клиентами, входящими в группу. Администратор в дереве объектов видит только своих клиентов, и имеет доступ к правилам глобального расписания, резервным копиям и задачам только своих клиентов.

Типы пользователей ALD Pro

В ALD Pro существуют следующие типы пользователей:

- Главный администратор
- Администратор
- Пользователь

ALD Pro, предназначен для централизованного управления физическими и виртуальными рабочими местами на базе операционной системы специального назначения «Astra Linux Special Edition» и может использоваться в организациях различного масштаба. ALD Pro может применяться в информационных (автоматизированных) системах, обрабатывающих общедоступную информацию и информацию ограниченного доступа.

ALD Pro предоставляет следующие базовые возможности:

- удаленное подключение к сессиям клиентов с портала управления;
- управление учетными записями пользователей и групп пользователей (создание, удаление, изменение параметров, изменение состава пользователей в группах);
- управление конфигурацией ОС на АРМ и серверах (установка/удаление программных пакетов, профиля пользователя, внешнего вида графической оболочки ОС);
- управление компьютерами и группами компьютеров (включение/исключение из домена, управление параметрами; создание/удаление/изменение состава компьютеров в группах);
- управление организационной структурой подразделений (создание и удаление подразделений, выстраивание иерархической структуры);
- управление групповыми политиками (создание, удаление, изменение параметров, назначение на организационные подразделения).
- добавление нескольких контроллеров домена;
- создание соглашения о репликации между контроллерами домена;
- настройка и конфигурация серверной группировки ALD Pro из портала управления;

Серверная группировка и клиенты ALD Pro могут размещаться на аппаратном оборудовании или на виртуальных машинах.

Функции администратора AIC

Администратор облачной платформы AIC выполняет следующие функции:

- Управление виртуализацией – создание и удаление ВМ, управление параметрами распределения ВМ
- Управление сетью – создание и удаление сетей, межсетевой экран
- Управление физическими серверами – настройка параметров оборудования, просмотр статуса оборудования, включение/выключение и перезагрузка оборудования

- Обслуживание компонентов платформы – обновление всех компонентов платформы, управление жизненными циклом ПО
- Управление учетными записями пользователей – создание и удаление учетных записей
- Управление правами доступа и к ресурсам платформы – настройка ролей пользователей с выбранным набором возможностей
- Управление безопасностью – разделение физических СХД между тенантами
- Генерация отчетов – алертинг, возможность устанавливать триггеры и получение нотификаций, или получение анализа по определенным алгоритмам
- Управление виртуальными машинами – настройка параметров автоматизации
- Управление дисками – создание, копирование и удаление дисков, включение и выключение дисков ВМ
- Просмотр статистики по ресурсам и пользователям – создание отчетов по использованию ресурсов, статистика SLA
- Мониторинг компонентов – формирование отчетов по компонентам, сбор и хранение метрик

В качестве виртуального оборудования выступают:

- серверы виртуализации;
- виртуальные сети;
- образы дисков ВМ;
- шаблоны ВМ;
- экземпляры ВМ.

Администратор AIC осуществляет управление следующим виртуальным оборудованием:

- серверами виртуализации;
- виртуальными сетями.

Установка

Порядок установки платформы, инструкция для установки и другие материалы необходимые для установки AIC базовой или стандартной конфигурации описаны в «Инструкции по установке» для базовой конфигурации , раздел 3.4 на странице продукта AIC.

Порядок обновления

В целях обеспечения соответствия требованиям безопасности информации в части устранения не декларированных возможностей и уязвимостей осуществляется ее техническая поддержка, предусматривающая выпуск очередного и оперативного обновлений.

Порядок выпуска и доведения обновлений до потребителей установлен в настоящем документе.

Информирование потребителей об окончании производства и (или) поддержки безопасности осуществляется с использованием контактной

информации, указанной в заключенных ранее лицензионных договорах (дополнениях к лицензионным договорам) и путем размещения соответствующей информации на сайте изготовителя. Информирование ФСТЭК России — официальным почтовым сообщением не позднее чем за один год до окончания производства и (или) поддержки безопасности.

Очередное обновление

Очередное обновление представляет собой заводские экземпляры, изготовленные в соответствии с конструкторской (программной) и технологической документацией, действующей на момент изготовления, с внесенными в нее порядком, установленным ГОСТ 2.503-2013, плановыми изменениями.

Очередное обновление решает следующий комплекс задач:

- устранение критических и некритических уязвимостей;
- обеспечение усовершенствования (модернизации) конструкции;

- поддержка современного оборудования;
- реализация новых функциональных возможностей;
- обеспечение соответствия актуальным требованиям безопасности информации;
- повышение удобства использования, управления компонентами AIC.

Очередное обновление предоставляется пользователям при заключении соответствующего лицензионного договора или дополнения к имеющемуся лицензионному договору, а также в соответствии с положениями «Лицензионного соглашения с конечным пользователем по использованию операционной системы специального назначения «Astra Linux Special Edition». Информация о выпуске очередного обновления для компонента размещается на официальном сайте изготовителя, а также доводится до лицензиатов (потребителей) с использованием контактной информации, указанной в заключенных ранее лицензионных договорах (дополнениях к лицензионным договорам).

Контроль целостности очередного обновления проводится следующим порядком:

- до установки — проведением проверки электронной подписи изготовителя (только для способа распространения по сетям связи);
- до установки — путем подсчета контрольной суммы установочного диска из комплекта поставки и сравнения с контрольной суммой, указанной в формуляре;
- после установки обновления — контроль целостности файлов программного обеспечения ПК СВ путем подсчета контрольных сумм файлов утилитой fly-admin-int-check с применением файла gostsums.txt, расположенного в корневом каталоге образа установочного диска (образа установочного диска).

В целях поддержания информационных (автоматизированных) систем в безопасном состоянии, обеспечения их работоспособности совместно с современным оборудованием и увеличения срока эксплуатации, рекомендуется на постоянной основе планировать и организовывать проведение мероприятий по применению очередного обновления ПК СВ.

Оперативное обновление

Оперативное обновление решает задачи:

1) оперативного устранения критических уязвимостей и уязвимостей высокого уровня опасности, находящихся в эксплуатации;

2) устранения функциональных недостатков;

3) совершенствование функциональных возможностей; и представляет собой бюллетень безопасности, который может быть доступен в виде:

- инструкций и методических указаний по настройке и особенностям эксплуатации, содержащих сведения о компенсирующих мерах или ограничениях по применению компонента при эксплуатации;

- отдельных программных компонентов из состава AIC, в которые внесены изменения с целью устранения уязвимостей, инструкций по их установке и настройке, а также информации, содержащей сведения о контрольных суммах всех файлов оперативного обновления;
- обновлений безопасности, представляющих собой файл с совокупностью программных компонентов из состава AIC, в которые внесены изменения с целью устранения уязвимостей, а также информации, содержащей сведения о контрольных суммах всех файлов обновлений безопасности, указания по установке, настройке и особенностям эксплуатации компонента с установленными обновлениями безопасности. Обновления безопасности представляют собой отдельные программные документы, не предусматривающие внесения изменений в комплект документации очередного обновления, характеристики которого подтверждены сертификатом соответствия требованиям безопасности информации.

Оперативное обновление содержит информацию об устраненных уязвимостях и предоставляется пользователям на безвозмездной основе.

Лицензиаты (потребители) оповещаются о выпуске и возможности получения обновления с использованием контактной информации, указанной в лицензионных договорах и дополнениях к ним, путем размещения соответствующей информации на официальном сайте и через личный кабинет.

Оперативное обновление не является самостоятельным программным изделием. Серийное производство и поставка (в том числе на материальных носителях) оперативного обновления не предусмотрены.

Доведение оперативного обновления до потребителей осуществляется изготовителем путем распространения по сетям связи. Источником получения оперативного обновления, подписанного усиленной квалифицированной электронной подписью изготовителя, является официальный сайт изготовителя.

Контроль целостности оперативного обновления и программного обеспечения после применения обновления осуществляется следующим порядком:

1. до установки обновления — путем проверки электронной подписи программного обеспечения обновления (образа установочного диска обновления или файлов, содержащих программное обеспечение с внесенными изменениями);
2. до установки обновления — проведением контроля целостности образа установочного диска оперативного обновления (или файлов, содержащего программное обеспечение с внесенными изменениями) путем подсчета его контрольной суммы и сравнения с контрольной суммой, указанной в бюллетене;
3. после установки обновления — проведением контроля целостности с использованием функции хэширования и автоматической сверки

полученного значения с эталонным, указанным в специальном файле gostsums.txt с контрольными суммами, входящем в состав оперативного обновления.

В рамках аттестации или при реализации мер по обеспечению целостности (меры группы «ОЦЛ») информационных систем, функционирующих с применением компонентов платформы, в целях подтверждения целостности, подлинности и неизменности сертифицированного программного обеспечения необходимо:

- проверить указание номера бюллетеня, содержащего оперативное обновление, в разделе «Сведения о бюллетенях»;
- контроль целостности установочного диска проводится путем подсчета контрольной суммы установочного диска из комплекта поставки и сравнения с контрольной суммой, указанной в формуляре;
- контроль целостности файлов программного обеспечения после применения оперативного обновления путем подсчета контрольных сумм файлов утилитой fly-admin-int-check с применением файла gostsums.txt, расположенного в корневом каталоге образа установочного диска (образа установочного диска).

Настройка программных компонентов ПК СВ Брест

Установка, первичная настройка и работа с компонентом описана в следующих документах:

Руководство администратора Часть 1 (описан порядок развертывания ПК СВ).

Включает в себя разделы:

- Установка программных компонентов
- Настройка хранилища
- Настройка сети
- Дополнительное конфигурирование службы сервера управления
- Мониторинг и учет

Руководство администратора Часть 2 (представлен порядок использования по назначению**)**

Включает в себя разделы:

- Инструменты управления ПК СВ Брест
- Пользователи и группы
- Управление экземплярами ВМ
- Управление серверами виртуализации и кластерами
- Настройка виртуальных сетей
- Планировщик

Инструкции по работе с ПК СВ Брест (первичная настройка и работа с ПК СВ)

Включает разделы:

- Управление виртуализацией
- Аутентификация пользователей AD
- Контекстуализация гостевых ОС
- Восстановление ВМ
- Статусы ВМ

Настройка сервера резервного копирования RuBackup

Первичная настройка происходит по руководству администратора СРК

Руководство администратора (описан порядок развертывания и первичной настройки СРК)

Включает в себя разделы:

- Конфигурация RuBackup
- Пользователи, группы, клиенты и группы клиентов
- Медиасерверы
- Хранилища резервных копий
- Стратегии резервного копирования
- Репозитории резервных копий

Настройка программного комплекса ALD Pro

Первичная настройка происходит по руководству администратора ALD Pro

Руководство администратора (описан порядок развертывания комплекса)

Включает в себя разделы:

- Развертывание контроллера домена
- Развертывание серверной группировки
- Добавление клиента
- Обновление
- Журналирование ПК