ПО «Базис.Storage Security». Руководство по эксплуатации

RU.НРФЛ.00006-01.97.01

Москва

09/12/2022

Содержание

1 Аннотация

Настоящий документ предназначен для технического администратора ПО и содержит инструкции по выполнению работ, необходимых для эксплуатации ПО.

2 Перечень. Термины и сокращения

Термин	Определение
Fiber Channel	Семейство протоколов для высокоскоростной передачи данных
iSCSI	(англ. Internet Small Computer System Interface) - протокол транспортного уровня для взаимодействия между системами хранения данных и серверами пользователей через IP-сети
LDAP	(англ. Lightweight Directory Access Protocol) - протокол прикладного уровня для доступа к службе каталогов
RAID	(англ. Redundant Array of Independent Disks) — технология виртуализации данных для объединения нескольких физических дисковых устройств в логический модуль для повышения отказоустойчивости и (или) производительности
USB	(англ. Universal Serial Bus) — «универсальная последовательная шина», последовательный интерфейс для подключения периферийных устройств к вычислительной технике
Коды Рида-Соломона	(англ. Reed–Solomon codes) — недвоичные циклические коды, позволяющие исправлять ошибки в блоках данных. Элементами кодового вектора являются не биты, а группы битов (блоки). Очень распространены коды Рида — Соломона, работающие с байтами (октетами).
ПО	Программное обеспечение
Пул	Логический объект СХД, объединяющий пространства нескольких физических накопителей в единое пространство хранения данных
СХД	Система хранения данных
ЦОД	Центр обработки данных

3 Введение

3.1 Назначение руководства

Настоящее руководство по техническому обслуживанию содержит инструкции по выполнению следующих работ:

- сопровождение и обслуживание ПО;
- диагностику, локализацию и устранение проблем.

3.2 Перечень эксплуатационных документов

Дополнительно к настоящему документу технические администраторы должны использовать следующие документы:

- «ПО «Базис.Storage Security». Руководство по установке. RU.НРФЛ.00006-01.96.01;
- «ПО «Базис.Storage Security». Руководство администратора RU.НРФЛ.00006-01.95.01.

3.3 Идентификационные данные ПО

Идентификационные данные ПО	**Программа для ЭВМ «Базис.Storage Security»**
Название документа	«ПО «Базис.Storage Security». Руководство по эксплуатации»
Обозначение документа	RU.НРФЛ.00006-01.97.01
Автор документа	ООО «БАЗИС»

3.4 Описание ПО

3.4.1 Назначение ПО

ПО «Базис.Storage Security» предназначено для организации систем хранения данных с высокой степенью доступности, производительности и целостности, формально представляющих собой сетевые блочные устройства хранения данных.

ПО «Базис.Storage Security» располагает встроенными функциями безопасности, обеспечивающими выполнение части мер защиты информации в соответствии с требованиями приказа ФСТЭК от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приведенными в п. 2.6 документа «Программное обеспечение «Базис.Storage Security». Технические условия», децимальный номер RU.НРФЛ.00006-01 90 01 ТУ.

ПО «Basis Storage Security» может применяться для защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, в государственных информационных системах 1 класса защищенности в соответствии с требованиями документа «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (введен в действие приказом ФСТЭК России № 17 от 11 февраля 2013 г.) и 1 уровня защищенности персональных в соответствии с документом «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных» (введен в действие приказом ФСТЭК России № 21 от 18 февраля 2013 г).

ПО «Базис.Storage Security» соответствует 4 (четвёртому) уровню доверия в соответствии с Требованиями по безопасности информации, устанавливающими уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденными приказом ФСТЭК России
от 2 июня 2020 г. № 76.

3.4.2 Структура ПО

ПО «Базис.Storage Security» включает в свой состав следующие подсистемы:

- подсистему виртуализации дискового массива СХД в виде блочных устройств (пулов и ресурсов, RAID массивов), в том числе с использованием алгоритмов на основе избыточных кодов Рида-Соломона;
- подсистему обновлений;
- подсистему кэширования;
- подсистему предоставления доступа к емкости СХД по каналам Fiber Channel и Ethernet;
- подсистему мониторинга и поддержания работоспособности СХД;
- подсистему обработки и отправки информации о событиях, возникающих в ходе работы СХД;
- подсистему сбора и предоставление статистической информации о работе СХД;
- подсистему предоставления интерфейса командной строки и веб-интерфейса для управления компонентами СХД и модулями в составе ПО «Базис.Storage Security»;
- подсистему безопасности;
- подсистему вспомогательных компонент для сборки образа ПО «Базис.Storage Security».

3.4.3 Функциональные возможности

Основные функции ПО

- виртуализация дискового массива СХД в виде блочных устройств (пулов и ресурсов, RAID массивов), в том числе с использованием алгоритмов на основе избыточных кодов Рида-Соломона;
- обновление ПО «Базис.Storage Security»;
- кэширование операций на чтение и запись;
- управление доступом к системе на основе ролевой модели и регистрация событий безопасности;
- предоставление доступа к емкости СХД по каналам Fiber Channel;
- мониторинг и поддержание работоспособности СХД;
- обработка и отправка информации о событиях, возникающих в ходе работы СХД;
- сбор и предоставление статистической информации о работе СХД;
- предоставление интерфейса командной строки и веб-интерфейса для управления компонентами СХД и модулями в составе ПО «Базис.Storage Security»;
- сборка образа ПО «Базис.Storage Security».

Безопасность

Безопасная работа ПО «Базис.Storage Security» основана на механизмах:

- разграничения доступа;
- регистрации событий безопасности.

ПО «Базис.Storage Security» содержит следующие меры защиты согласно требованиями документа «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (введен в действие приказом ФСТЭК России № 17 от 11 февраля 2013 г.):

- управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей (УПД.1, в части определения типа учетных записей, заведения, а также осуществления оповещения администратора информационной безопасности об изменении сведений о пользователях);
- реализация необходимых методов (ролевой) и правил разграничения доступа (УПД.2, в части реализации ролевого метода управления доступом, предусматривающего управление доступом субъектов доступа к объектам доступа;
- ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы (УПД.9, в части реализации механизма ограничения на число параллельных (одновременных) сеансов (сессий), основываясь на идентификаторах пользователей и (или) принадлежности к определенной роли, в частности для привилегированных учетных записей (администраторов) количество параллельных (одновременных) сеансов (сессий) от их имени с разных устройств (средств вычислительной техники) не должно превышать двух);
- блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу (УПД.10, в части реализации механизма блокирования доступа пользователя к ПО «Basis Storage Security» после установленного оператором времени его бездействия);
- разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации (УПД.11, в части реализации запрета действий пользователей до прохождения ими процедур идентификации и аутентификации; в части разрешения следующих действий пользователей до прохождения ими процедур идентификации и аутентификации: изменение языка интерфейса, просмотр пользовательского соглашения);
- управление взаимодействием с иными системами (УПД.16, в части предоставления доступа к информационной системе только авторизованным (уполномоченным) пользователям, определения системных учетных записей, используемых в рамках данного взаимодействия);

- определение событий безопасности, подлежащих регистрации, и сроков их хранения (РСБ.1, в части регистрации следующих событий: вход и попытки входа субъектов в ПО «Basis Storage Security»; заведение и активация (блокирование) пользователей; изменение правил разграничения доступа, запуск (завершение) заданий, связанных с обработкой защищаемой информации);
- определение состава и содержания информации о событиях безопасности, подлежащих регистрации (РСБ.2, в части обеспечения возможности идентификации: типа события; даты и времени события; результата события; субъекта доступа, связанного с событием. Также в части обеспечения записи в журнал безопасности следующей информации при регистрации входа: дата и время, результат; идентификатор. В части обеспечения записи в журнал безопасности следующей информации при регистрации запуска (завершения) пользователем заданий, связанных с обработкой защищаемой информации: дата и время, имя (идентификатор) пользователя, запустившего задание, результат запуска);
- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения (РСБ.3, в части обеспечения возможности выбора администратором информационной безопасности событий безопасности, подлежащих регистрации в текущий момент времени, генерации записей регистрации для событий безопасности подлежащих регистрации);
- генерирование временных меток и (или) синхронизация системного времени в информационной системе (РСБ.6, в части осуществления получения временных меток, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в информационной системе посредством применения внутренних системных часов операционной системы среды функционирования);
- защита информации о событиях безопасности (РСБ.7, в части предоставления доступа к записям журналов безопасности только администратору информационной безопасности).

Подробное описание функциональных возможностей ПО приведено в документе «ПО «Базис.Storage Security». Руководство администратора».RU.НРФЛ.00006-01.95.01.

Ролевая модель

При управлении СХД используется ролевая модель доступа, определяющая зоны ответственности пользователей и доступные им функции в интерфейсах управления СХД.

Для всех пользователей СХД используется один тип учетной записи, которая может быть наделена одной из следующих ролей:

- роль **monitor** — с возможностью просмотра информации о конфигурации и состоянии системы, ее логических объектов и аппаратных компонентов, а также изменения пароля учетной записи;
- роль **admin** — с возможностью использования всех пользовательских функций в интерфейсах управления;
- роль **service** – аналогична admin, но имеет привилегированный доступ к утилитам диагностики и управления, служит для обслуживания системы производителем или авторизованными сервисными партнерами;
- **host** – роль-объект для доступа к данным, хранящимся на СХД. Доступ осуществляется через системный низкоуровневый протокол iSCSI;
- **expert** – роль для экстренного восстановления системы силами производителя (например в случае сбоя LDAP и невозможности доступа к системе).

Для доступа к этой роли требуется:

1. Получить доступ в ЦОД, где установлена СХД.
2. Получить доступ к стойке, в которой размещается СХД.
3. Идентифицировать СХД.
4. Физически вытянуть контроллерное шасси СХД из стойки.
5. Вскрыть крышку контроллерного шасси СХД.
6. Подключить рабочую станцию пользователя к интерфейсу USB.
7. Ввести учетные данные.
8. Произвести работы.

Ввод параметров учетной записи производится при подключении к интерфейсу управления.

4 Общие указания

Для реализации функций безопасности среды функционирования ПО «Базис.Storage Security» должны выполняться следующие действия:

- необходимо регулярное обновление всех сред функционирования ПО «Базис.Storage Security» до актуальных версий с применением всех необходимых патчей безопасности с официальных сайтов разработчиков сред функционирования;
- компоненты операционной системы и сред функционирования ПО «Базис.Storage Security» должны быть максимально ограничены. Компоненты, которые не участвуют в функционировании ПО «Базис.Storage Security», должны быть отключены;
- должно обеспечиваться предотвращение несанкционированного доступа к идентификаторам и паролям администраторов среды виртуализации, которые необходимы для управления и технической поддержки среды функционирования ПО «Базис.Storage Security»;
- необходимо использовать на серверах, где развернута среда функционирования ПО «Базис.Storage Security», в качестве средств защиты информации от несанкционированного доступа, сертифицированных ФСТЭК России версий операционных систем с установленными обновлениями или наложенных средств защиты информации, прошедших сертификацию по требованиям безопасности информации в системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00;
- должна быть обеспечена физическая сохранность серверной платформы с установленным ПО «Базис.Storage Security» и исключение возможности физического доступа к ней посторонних лиц;
- каналы передачи данных ПО «Базис.Storage Security» должны быть либо расположены в пределах контролируемой зоны и защищены с использованием организационно-технических мер, либо, в случае их выхода за пределы контролируемой зоны, должны быть защищены путем применения средств криптографической защиты информации, сертифицированных в системе сертификации ФСБ России.

4.1 Требования к составу и квалификации обслуживающего персонала

Для успешного освоения администрирования ПО «Базис.Storage Security» необходимо обладать высоким уровнем квалификации в области администрирования системного ПО и практическим опытом выполнения работ по установке, настройке и администрированию программных средств, применяемых в ПО «Базис.Storage Security», а также иметь профессиональные знания и практический опыт в области системного администрирования.

4.2 Действия по безопасной установке и настройке

4.2.1 Общие сведения о сборке

В компиляции и сборке компонентов программного обеспечения СХД используются три репозитория (см. Рисунок 1):

1. Репозиторий исходных кодов компонентов.
2. Репозиторий docker-образов.
3. Репозитории бинарных компонентов (rpm).

Рисунок 1— Процесс сборки и компиляции ПО «Базис.Storage Security»

Компиляция программного обеспечения СХД выполняется на основе исходных кодов с помощью docker-образов. В результате компиляции формируются выходные rpm-пакеты.

Подробное описание установки ПО приведено в документе ПО «Базис.Storage Security» «Руководство по установке». RU.НРФЛ.00006-01.96.01.

4.3 Режимы работы ПО

ПО «Базис.Storage Security» функционирует в следующих режимах:

- штатный режим, при котором обеспечивается выполнение задач в объеме функций, при работоспособности всех функций;
- сервисный режим, необходимый для проведения обслуживания, реконфигурации и пополнения технических и программных средств ПО «Базис.Storage Security» новыми компонентами;
- аварийный режим работы.

В штатном режиме функционирования ПО «Базис.Storage Security» обеспечивает следующий режим работы: доступность функций ПО «Базис.Storage Security» в режиме — 24 часа в день, 7 дней в неделю (24×7). Круглосуточный режим работы системы не требует организации круглосуточной работы пользователей и допускает работу пользователей ПО «Базис.Storage Security» в соответствии со штатным расписанием.

В сервисном режиме ПО «Базис.Storage Security» обеспечивает возможность проведения следующих работ:

- техническое обслуживание;
- модернизацию аппаратно-программного комплекса;
- устранение аварийных ситуаций.

Регламентные работы производятся с учетом требований о доступности ПО «Базис.Storage Security».

Функционирование ПО «Базис.Storage Security» при отказах и сбоях серверного общесистемного и специального программного обеспечения, и оборудования, в том числе структурных узлов

ПО «Базис.Storage Security», не предусматривается.

4.4 Аварийные ситуации

4.4.1 Действия в случаях обнаружении несанкционированного вмешательства в данные

Несанкционированное вмешательство обнаруживается при помощи протокола нарушений безопасности.

В случаях обнаружения несанкционированного вмешательства в данные, необходимо установить логин пользователя, под которым была произведена аутентификация, затем сменить пароль для этого пользователя и проинформировать пользователя о смене пароля.

4.4.2 Действия в других ситуациях

В других аварийных ситуациях необходимо обратиться в сервисную службу:

Электронный адрес: **support@**basistech.ru[1]

1 http://basistech.ru/

5 Требования к техническим средствам

5.1 Требования к аппаратной части

Функционирование ПО «Базис.Storage Security» должно быть построено на основе сервисной архитектуры, включающей следующие сервисы:

- сервис обработки запросов файлового хранилища;
- сервис обработки запросов блочного хранилища;
- сервис обработки запросов холодного архива;
- сервисы управления;
- сервис координации контроллеров СХД;
- сервис конфигурации параметров контроллеров СХД;
- сервис управления логическими группами (пулами) дисков;
- сервис управления ресурсами;
- сервис мониторинга и сбора метрик компонент СХД

ПО «Базис.Storage Security» должно размещаться на специализированном оборудовании, оснащенном контроллером хранения данных и подключенным к нему дисковым накопителям.

В качестве хост-серверов, подключаемых к СХД, должен выступать сервер с одной из операционных систем, приведенных ниже:

- CentOS 7.6/8;
- SUSE 12 SP5/15/15SP1;
- RHEL 7.6/7.7/8.0;
- Ubuntu 18.04 LTS/18.04 1-5 LTS/20.04 LTS/20.04 1 LTS/20.10;
- Windows Server 2016/2019;
- VMware vSphere 6.5/6.7/7.

5.2 Требования к программно-техническому обеспечению

Для функционирования ПО «Базис.Storage Security» необходим состав программно-аппаратных средств, представленный в таблице 1.

Таблица 1 – Состав программно-аппаратных средств для работы ПО «Базис.Storage Security»

№	Название	Количество
1.	Контроллеры хранения	2
2.	Контроллерное шасси	1
3.	Дисковые полки расширения до	4
4.	Минимум/максимум накопителей	3/386
5.	Процессоры	4
6.	Кэш-память по умолчанию / опция расширения	512 ГБ/1024 ГБ
7.	Интерфейс подключения накопителей	SAS 3.0, PCI Express 3.0
8.	Максимальное количество портов FC	32
9.	Максимальное количество портов Ethernet	16

№	Название	Количество
10.	Поддерживаемые типы накопителей	NVMe SSD 1 DWPD 1.92 TB, 3.84 TB, 7.68 TB, 15 TB U.2 NVMe SSD 3 DWPD 1.6 TB, 3.2 TB, 6.4 TB U.2 SAS SSD 1 DWPD 1.92 TB, 3.84 TB, 7.68 TB, 15.36 TB, 30.72 TB 2,5” SAS SSD 3 DWPD 1.6 TB, 3.2 TB, 6.4 TB 2,5” SAS 10K 1.8 TB, 2.4 TB 2,5” NL-SAS 7.2K 6 TB, 10 TB, 12 TB, 14 TB, 16 TB 3,5”

6 Описание функций

Описание совместного функционирования технических средств и ПО, описание организации входных и выходных данных, используемых при обслуживании технических средств и описание взаимодействий устройств с ПО приведено в эксплуатационных документах:

«ПО «Базис.Storage Security». Руководство по установке. RU.НРФЛ.00006-01.96.01;

«ПО «Базис.Storage Security». Руководство администратора. RU.НРФЛ.00006-01.95.01.