



СТР

ГиперСфера

**Программное обеспечение для построения
отказоустойчивых кластеров**

Описание архитектуры

Контактная информация

115280, г. Москва,
ул. Ленинская Слобода, д. 26
эт. 5, пом. XXXII, ком. 62
+7 (495) 646-85-11
E-mail: maintenance@str-technologies.com
<https://str-technologies.com/>

Авторское право

ООО «СТР»
<https://str-technologies.com/>
© 2008 – 2024 ООО «СТР»

Версия документа

Ноябрь 10, 2024

Настоящий документ является собственностью ООО «СТР» (далее – «СТР») и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения «СТР».

Документ может быть изменен без предварительного уведомления.

Содержание

1.	Термины и определения.....	4
2.	Обозначения и сокращения	5
3.	Общие положения.....	6
4.	Цель и задачи	6
5.	Описание архитектуры	7
6.	Режимы работы.....	8
6.1	Режим высокой доступности	8
6.2.	Режим отказоустойчивости	9
7.	Обоснование архитектуры	9
7.1.	Операционная система.....	9
7.2.	Сетевые соединения.....	10
7.3.	Архитектура хранилища	10
7.4.	Методы обеспечения безопасности	10
8.	Требования к инфраструктуре	11
8.1.	Поддерживаемые серверы	12
8.2.	RAM	12
8.3.	Дисковое пространство	12
8.4.	Сеть	12
8.5.	IP-адреса	13

1. Термины и определения

В настоящем документе используются термины с соответствующими определениями, представленные в таблице 1.

Таблица 1. Термины и определения

№	Термин	Определение
	Нода	Отдельный узел сети, выполняющий обработку данных наравне с другими узлами, принимая на себя нагрузку при выходе из строя другой узла.
	Том	Пространство хранения, в котором хранится том и копии файлов, каталогов файловой системы (образ ОС), связанные с этим томом.

2. Обозначения и сокращения

В настоящем документе используются сокращения, представленные в таблице 2.

Таблица 2. Сокращения и расшифровка

№	Сокращение	Значение
	ВД	Высокая доступность
	ВМ	Виртуальная машина
	ПО	Программное обеспечение
	ФМ	Физическая машина
	ЦП	Центральный процессор

3. Общие положения

В настоящем документе приведено описание архитектуры программного обеспечения для построения отказоустойчивых кластеров ГиперСфера (далее – ПО).

Описание архитектуры ПО построено в два этапа:

На первом этапе представлено обобщенное описание существующих функциональных модулей и подсистем, а также инфраструктуры ПО.

На втором этапе представлено обоснование выбранных компонентов ПО с точки зрения производительности, надежности и безопасности, направленные на нарушение работоспособности.

В результате приведения обоснования будут сделаны выводы, что архитектура ПО в полном объеме обеспечивает ее производительность, надежность и безопасность.

4. Цель и задачи

Целью настоящего документа является описание и обоснование архитектуры ПО ГиперСфера, предназначенный для построения отказоустойчивых кластеров.

Для достижения цели в настоящем документе решены следующие основные задачи:

1. Дано описание основных компонентов ПО и их взаимодействие.
2. Представлено описание основного функционала ПО и возможности его интеграции с другими системами.
3. Обосновано обеспечение внутренней безопасности модулей ПО.

5. Описание архитектуры

Общая схема работы ПО представлена на рисунке 1.



Рисунок 1. Архитектура ПО

Описание и назначение модулей ПО ГиперСфера представлено в таблице 3.

Таблица 3. Описание функциональных модулей

№	Наименование	Описание
	Модуль графического интерфейса	Визуализация данных и осуществление взаимодействия пользователя с функциональными модулями ПО
	Модуль конфигурации системных настроек	Выполняет управление настраиваемыми системными параметрами

№	Наименование	Описание
	Модуль управления физическими машинами	Позволяет осуществлять управление физическими нодами и их ресурсами
	Модуль управления виртуальными машинами	Осуществляет управление виртуальными машинами, томами, группами хранилищ, снимками ОС и виртуальными дисками.
	Модуль журналирования	Сбор данных по системным оповещениям, аудит и поддержка.
	Модуль хранения данных	Хранение данных по данным в системе

6. Режимы работы

6.1. Режим высокой доступности

ПО ГиперСфера обеспечивает два определяемых пользователем уровня доступности для виртуальных машин: высокая доступность (далее – ВД) и отказоустойчивость.

В режиме высокой доступности ПО автоматически обнаруживает, изолирует и обрабатывает большинство аппаратных сбоев, тем самым поддерживая работу ваших приложений. Благодаря технологии удаленной поддержки программное обеспечение уведомляет в разделе панели управления о различных проблемах, указывая тип неисправности и ее точное местоположение. Эта комбинация технологий автоматического обнаружения неисправностей, изолирования и удаленной поддержки обеспечивают быстрый доступ к экспертной поддержке технических специалистов и быстрое решение проблемы.

При включении режима высокой доступности обеспечиваются базовые функции отказоустойчивости и восстановления, при этом некоторые сбои требуют (автоматической) перезагрузки ВМ для восстановления и возврата к режиму ВД:

- Устраняет время простоя из-за многих, но не всех отказов ЦП, памяти, ошибок ввода-вывода или других неисправностях

физических машин (ФМ).

- Обрабатывает сбои без вмешательства ИТ специалистов.
- Обеспечивает непрерывную активную проверку всех компонентов.
- Обеспечивает постоянное резервирование и восстановление.

Режим ВД подходит для приложений, которые могут допускать случайные прерывания на несколько минут.

6.2. Режим отказоустойчивости

В режиме отказоустойчивости ПО ГиперСфера обеспечивает работу приложения без простоев во время сбоя. Уровень доступности ВМ выбирается при создании или импорте виртуальной машины в панели управления.

В режиме отказоустойчивости ПО прозрачно защищает приложение, создавая резервную среду для виртуальной машины, работающей на двух ФМ. С идентичным экземпляром выбранной ВМ на втором хосте ПО ГиперСфера обеспечивает защиту виртуальной машины в режиме отказоустойчивости.

При включении режима отказоустойчивости прозрачно защищается ВМ от всех сбоев, без простоев, и режим отказоустойчивости обеспечивает следующие функции:

- Устраняет времяостоя из-за любого отказа ЦП, ошибок памяти, ввода-вывода или других неисправностях ФМ;
- Обрабатывает сбои без вмешательства ИТ специалистов;
- Обеспечивает отсутствие потери данных;
- Обеспечивает непрерывную активную проверку всех компонентов;
- Обеспечивает постоянное полное резервирование и восстановление.

7. Обоснование архитектуры

7.1. Операционная система

Система реализована на операционной системе РЕД ОС 7.3, российской операционной системе семейства Linux, предоставляющей универсальную среду для использования прикладного программного обеспечения. РЕД ОС включена в реестр российского программного обеспечения. Сертифицирована ФСТЭК России.

7.2. Сетевые соединения

ПО ГиперСфера использует порт 443 в локальном брандмауэре для связи по HTTPS, порт 22 для ssh и порт 5900-59nn для каждого активного VNC, связанного с каждой виртуальной машиной. Межсетевые экраны должны разрешать трафик через соответствующие порты.

Межсетевые экраны должны разрешать виртуальным машинам связываться с компьютерами службы кворума, используя порт UDP 4557.

Сети Ethernet обеспечивают пути для связи между двумя физическими машинами (ФМ) или узлами системы. Основные типы сетей Ethernet:

- Одна сеть A-Link должна быть частной сетью (priv0), соединяющей два модуля ГиперСфера ФМ.
- Корпоративные сети позволяют вашим приложениям подключаться к существующей сети. Единая корпоративная сеть должна быть управляющая сеть (ibiz0, иногда называемая network0), которая подключается к панели управления ГиперСферы и использует кворум-серверы.

7.3. Архитектура хранилища

RAID контроллеры в системе ГиперСфера создают логические диски из физических дисков системы. Логические диски собираются в группы хранения. Логические диски содержат системные тома ГиперСферы и тома виртуальных машин.

ПО ГиперСфера поддерживает внутренние диски. Две физические машины в системе ГиперСфера могут иметь разные емкости хранилища, однако системе доступна только меньшая емкость. Например, если у одной ФМ есть 1 ТБ хранилища в группе хранения, а другая имеет 2 ТБ хранилища в той же группе хранения, то только 1 ТБ доступны системе ГиперСфера для этой группы хранения.

7.4. Методы обеспечения безопасности

Методы обеспечения безопасности ПО представлены в таблице 6.

Таблица 4. Методы обеспечения безопасности Системы

№	Тип угрозы	Методы защиты
	Нарушение работы модулей ПО	<ul style="list-style-type: none">– Оповещение администратора ПО по электронной почте, в мессенджере, события в SIEM и в графическом интерфейсе системы
	Несанкционированный доступ к ПО	<ul style="list-style-type: none">– Авторизация по идентификационным данным: логин/пароль– Временная блокировка и оповещение администратора ПО при превышении попыток входа в Систему– Блокировка неиспользуемых учетных записей– Периодическая принудительная смена пароля для учетных записей
	Удаленное управление ресурсами Системы	<ul style="list-style-type: none">– SSH доступ имеет строгий плейбук– SSL сертификат
	Перехват данных во время передачи (MITM)	<ul style="list-style-type: none">– Передача данных осуществляется по защищенному протоколу HTTP(S)

8. Требования к инфраструктуре

Минимальные требования к аппаратному обеспечению описаны в таблице 7.

Таблица 5. Минимальные требования к аппаратному обеспечению

№	Параметры	Значение
	CPU	Два x86 сервера

	RAM, ГБ	8
	HDD, ТВ	22
	SSD, ТВ	0,5
	Сеть	1000 Мбит/с (4 шт.)

Для ПО ГиперСфера требуется два хост-сервера x86-64 (физические машины (ФМ) или узлы), которые могут поддерживать несколько виртуальных машин (ВМ) и компьютер удаленного управления (то есть ПК общего назначения), который может запустить панель управления ГиперСфера. Требования к аппаратному обеспечению системы ГиперСфера приведены ниже.

8.1. Поддерживаемые серверы

Программное обеспечение ГиперСфера работает на любых системах, перечисленных в каталоге оборудования Red Hat® Linux, которые поддерживают RHEL 7.x и любой из поддерживаемых процессоров, перечисленных в системных требованиях к физическому компьютеру.

Второй компьютер с идентичными процессорами требуется для использования в качестве резервного сервера для гостевой виртуальной машины (ВМ), защищенные программным обеспечением ГиперСфера. ЦП для каждого хост-компьютера должны включить аппаратную поддержку виртуализации в утилите настройки микропрограммы (BIOS или UEFI).

8.2. RAM

Рекомендуется не менее 8 ГБ оперативной памяти (физической памяти).

8.3. Дисковое пространство

Поддерживаются внутренние диски. Требуется минимум два диска на физическую машину. 477 МБ требуется на каждом внутреннем логическом диске для основной операционной системы РЕД ОС 7.3. Кроме того, 22 ГБ требуется на двух внутренних логических дисках для системных данных ГиперСфера, включая журналы.

8.4. Сеть

Минимальная конфигурация сети включает два порта: один для A-link и один для общего управления/корпоративный. Оптимальная конфигурация сети включает два сетевых порта 10-GbE для A-Link (один из которых также служит priv0, частная сеть), сетевой интерфейс для сети управляемой, и столько же и столько деловых/производственных портов, сколько может понадобиться гостевым виртуальным машинам. Если вы планируете запустить несколько виртуальных машин, рассмотрите возможность добавления пар A-Links, всего до четырех поддерживаемых пар.

8.5. IP-адреса

ПО ГиперСфера должно иметь статический IP-адрес IPv4, назначенный для использования программным обеспечением. Необходимо получить IP-адреса для первичного и вторичного серверов DNS, а также информацию о шлюзе и маске подсети для вашей панели управления от администратора ИТ-сети.