УТВЕРЖДАЮ

Генеральный директор
АО «Иридиум»

Ю.С. Денисенко
«29» августа 2024 г.

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС (ПАК) «ИРИДИУМ-АЛЬТАИР»

Функциональные характеристики

УГСФ.468313.001Д2

Листов 12

2024

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

АННОТАЦИЯ

Настоящий документ включает в себя описание функциональных характеристик Программно-аппаратного комплекса “Иридиум-Альтаир” УГСФ.468313.001 (далее – ПАК “Иридиум-Альтаир”, изделие), разработанного АО “Иридиум”.

Программно-аппаратный комплекс “Иридиум-Альтаир” является гиперконвергентной системой, состоящей из программного комплекса “Иридиум” и вычислительного сервера Альтаир Z. Поддерживает развертывание виртуальных машин с гостевыми ОС семейства Windows и Linux, подключение хранилищ и создание виртуальных сетей.

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Основные сведения о ПАК “Иридиум-Альтаир”

ПАК “Иридиум-Альтаир” предназначен для формирования защищенной виртуальной информационно-коммуникационной среды.

Изделие является комплексным решением для создания как классических конвергентных, так и гиперконвергентных виртуальных сред. Изделие поддерживает работу с классическими системами хранения данных (СХД) по протоколам Fibre Channel, iSCSI, NFS.

Сфера применения ПАК “Иридиум-Альтаир” – как предприятия госсектора, объекты ГИС, КИИ, ИСПДн, так и коммерческие предприятия.

1.2 Комплектность изделия

Состав изделия приведен в таблице 1.1.

Таблица 1.1 – Состав ПАК “Иридиум-Альтаир”

№ п/п	Наименование основных составных частей	Обозначение	Примечание
1	Аппаратные средства: Вычислительный узел Альтаир 1x10 Вычислительный узел Альтаир 2x24	 ВНРЯ.466219.006 ВНРЯ.466219.004	Вычислительные узлы Альтаир внесены в Реестр российской промышленной продукции (запись в реестре от 21.12.2023 № 10514134 и № 10514136)
2	Программный комплекс «Иридиум»	RU.УГСФ.00001-01	Программный комплекс “Иридиум” зарегистрирован в Реестре российского программного обеспечения (запись в реестре от 01.03.2023 №16819).
3	Комплект документации	УГСФ.468313.001ВЭ	Поставляется в электронном виде

1.3 Функциональные возможности

ПАК “Иридиум-Альтаир” предоставляет следующие возможности:

— поддержку встроенных контролеров для обеспечения установки компонентов виртуализации на локальные диски серверов;
— поддержку сетевых карт;
— поддержку FC HBA адаптеров для подключения гипервизоров к сети заказчика;
— поддержку всего объема оперативной памяти сервера для использования виртуальными машинами в гипервизоре;

- поддержку ОС в режиме гостя для обеспечения миграции сервисов заказчика на новую систему виртуализации;
- наличие драйверов виртуального оборудования под необходимые ОС: дисковый драйвер, сетевой драйвер, поддержка процессоров;
- поддержку необходимых для обеспечения работы сервисов заказчика объёмов ресурсов, выделяемых виртуальной машине со стороны гипервизора;
- миграцию виртуальных машин с существующей у заказчика системы виртуализации;
- миграцию существующей виртуальной машины с различными ОС;
- создание, удаление виртуальных машин (ВМ);
- настройка оборудования ВМ (CPU/Mem/диски/CD-ROM);
- подключение к консоли ВМ;
- вывод общей информации о ВМ;
- мониторинг загрузки ресурсов ВМ;
- клонирование ВМ;
- создание, управление, удаление виртуальных сетей;
- виртуализацию сети на уровне l2-l4;
- возможность агрегации сетевых устройств из интерфейса управления (web-интерфейса);
- создание, управление, удаление хранилищ;
- создание и подключение виртуальных дисков;
- поддержку Thin Provision дисков на файловых и блочных хранилищах
- создание, управление образов ISO, библиотек;
- создание папки в хранилище;
- загрузка файла в папку хранилища;
- удаление, перемещение, копирование файлов в хранилище;
- создание файлового хранилища NFS;
- мониторинг загрузки ресурсов хоста;
- мониторинг загрузки ресурсов виртуальных машин;
- вывод предупреждений для администратора;
- поддержка интеграции с системой мониторинга (zabbix).

2 АРХИТЕКТУРА ПАК “ИРИДИУМ-АЛЬТАИР”

2.1 Аппаратная составляющая

2.1.1 Высокая производительность

• Поддержка новейших процессоров Intel Xeon Scalable 3-го поколения (архитектура Ice Lake) мощностью до 270 Вт;

• 16 слотов для модулей памяти DIMM DDR4 3200 МГц с возможностью расширения полного объема ОЗУ до 4 Тбайт.

2.1.2 Хорошая расширяемость

• До 24 накопителей формфактора 2,5 дюйма (SFF), в том числе до 8 накопителей U.2 NVMe и 2 накопителя SFF Slimline (высотой до 7 мм);

• Поддержка шины PCIe четвертого поколения;

• Поддержка карт расширения OCPv3.

2.1.3 Высокая надежность

• Блоки питания с возможностью горячей замены и резервированием по схеме 1+1;

• Вентиляторы охлаждения с возможностью горячей замены и резервированием по схеме 2+1;

• Модули ОЗУ с поддержкой кодов коррекции ошибок (исправление единичной ошибки без влияния на работу системы);

• Возможность резервирования сетевого интерфейса управления;

• Система самодиагностики аппаратного и встроенного программного обеспечения;

• Возможность восстановления встроенного программного обеспечения в случае сбоя или нарушения целостности кода;

• Регулярный выпуск обновлений встроенного программного обеспечения.

2.1.4 Удобство в эксплуатации и обслуживании

• Интегрированный контроллер BMC с поддержкой протоколов IPMI 2.0 и Redfish 1.8 для интеграции с централизованными системами управления и мониторинга;

• Инвентаризация установленного оборудования через интерфейс управления;

• Настраиваемая отправка уведомлений администратору;

• Поддержка аутентификации и авторизации через OpenLDAP или Active Directory.

2.1.5 Учет особых требований заказчика

• Возможность гибкого конфигурирования аппаратного обеспечения под конкретные задачи;

• Опциональная физическая защита от несанкционированного доступа к накопителям и мониторинг вскрытия корпуса;

• Поддержка отечественных операционных систем.

2.1.6 Оборудование российского происхождения

• Включено в Единый реестр российской радиоэлектронной продукции согласно Постановлению Правительства РФ от 10.07.2019 N 878;

• Программное обеспечения UEFI BIOS и BMC разработано в России и включено в Единый реестр российского программного обеспечения.

2.2 Особенности программного комплекса

При создании ПК «Иридиум»учитывался и максимально приближен пользовательский опыт администратора к таковому для продукта VMware vSphere. Веб-интерфейс системы оркестрации и одиночных хостов виртуализации ПК «Иридиум» максимально точно соответствует веб-интерфейсу VMware vCenter (система оркестрации в продукте VMware vSphere). По приблизительным оценкам в Российской Федерации более 100 тысяч специалистов по VMware vSphere, подготовленных за годы присутствия компании VMware на российском рынке. Эти специалисты могут начать работать с ПК «Иридиум», не являясь при этом глубокими специалистами по ОС Linux, и не проходя длительное 1-2-годичное переобучение (что требовалось бы для эксплуатации программных продуктов наших конкурентов).

2.2.1 Защищенная специализированная закрытая ОС

Разработка продукта берет начало в 2009 году. ПК «Иридиум» изначально задумывался как защищенная сертифицированная отечественная система виртуализации. В процессе разработки продукта были разработаны более 150 патчей ядра операционной системы (как функциональные, так и патчи информационной безопасности). Из операционной системы было исключено все ПО, которое не имеет отношения к виртуализации, что сократило до минимума возможную площадь атаки. Был исключен менеджер пакетов с целью предотвращения установки ПО из сторонних репозиториев Open Source. С целью предотвращения запуска любого стороннего не одобренного вендором ПО был реализован динамический контроль исполняемого кода. Это предполагает проверку цифровой подписи при попытке

запуска любого исполняемого кода (как бинарных файлов, так и модулей ядра). При неуспешной проверке цифровой подписи или ее отсутствии исполняемый код не запускается.

Таким образом, была разработана специализированная закрытая защищенная операционная система – гипервизор 1-го типа, которая устанавливается непосредственно на физические серверы. Ключевые особенности нашей специализированной закрытой защищенной операционной системы:

- Минимальная площадь атаки за счет исключения ПО, не относящегося к задачам виртуализации,
- Отсутствие возможности запуска стороннего не одобренного вендором ПО за счет динамического контроля исполняемого кода,
- Реализация встроенных средств защиты информации (СЗИ).

Вышеперечисленные особенности являются критичными для защищенной системы виртуализации, поскольку защищенность любой ИТ-системы не может быть выше защищенности платформы виртуализации, на которой развернута данная ИТ-система. В случае применения ПК «Иридиум» возможно развертывание государственных информационных систем (ГИС) разных классов защищенности на одном и том же кластере и даже на одном и том же хосте виртуализации. Также за счет применения встроенных СЗИ допускается одновременное развертывание как сертифицированных, так и несертифицированных гостевых ОС на одном и том же хосте виртуализации. В защищенной операционной системе полностью исключается взлом гипервизора через гостевую ОС.

Платформа виртуализации обладает сертификатом ФСТЭК как средство защиты информации (СЗИ), а также сертификатом Министерства обороны РФ.

2.2.2 Виртуальный коммутатор

В состав ПК «Иридиум» входит виртуальный сетевой коммутатор, который не основан на Open vSwitch, а целиком и полностью является собственной разработкой. Это позволило максимально приблизить архитектуру виртуального коммутатора ПК «Иридиум» к архитектуре виртуального коммутатора VMware vSphere, и реализовать функционал виртуального коммутатора на уровне VMware vSphere.

Виртуальный коммутатор в ПК «Иридиум» является распределенным, что позволяет осуществлять централизованное управление сетевым функционалом платформы виртуализации.

2.2.3 Файловая система

В ПК «Иридиум» была полностью «с нуля» переписана подсистема ввода/вывода в части взаимодействия с СХД, а также была разработана кластерная файловая система – аналог VMware VMFS, по функционалу не уступающая VMware VMFS. Архитектура данной псевдо-файловой системы предполагает, что данные хранятся непосредственно в виде блоков на разделяемых LUN СХД, а наименования файлов и папок хранятся в виде метаданных. Сама прослойка файловой системы фактически отсутствует. Благодаря этому удалось достичь высоких показателей производительности подсистемы ввода/вывода - по результатам тестов, проведенных нашими заказчиками, производительность псевдо-файловой системы на 18-36% превосходит производительность файловой системы VMFS от VMware, на том же самом аппаратном обеспечении.

2.2.4 Программно-определяемая СХД «Шторм»

В состав ПК «Иридиум» входит распределенная программно-определяемая СХД «Шторм», которая может быть использована для построения гиперконвергентных кластеров хранения на базе локальных дисков, установленных в физические хосты.

В гиперконвергентном кластере один и тот же хост виртуализации может одновременно участвовать в создании распределенного кластера хранения, и запускать продуктивные виртуальные машины.

Другой вариант – создание программно-определяемого кластера хранения на выделенных хостах (конвергентный кластер), и предоставление пространства хранения данного конвергентного кластера хостам виртуализации и другим системам по протоколам iSCSI, NFS, S3. Ближайший аналог программно-определяемой СХД «Шторм» – продукт VMware vSAN.

2.2.5 Система оркестрации

Весь интеллектуальный функционал системы виртуализации реализован в системе оркестрации, которая была разработана полностью «с нуля» и не основана ни на каких опенсорсных аналогах. Пример функционала, который реализован в системе оркестрации:

- Живая миграция ВМ между хостами виртуализации,
- Живая миграция виртуальных дисков ВМ между хранилищами,
- Отказоустойчивость хостов виртуализации (при падении хоста все ВМ автоматически перезапускаются на других хостах кластера),

- Отказоустойчивость самой системы оркестрации,
- Автоматическая балансировка нагрузки на хосты виртуализации,
- Многие другие функции.

Полнота функционала платформы виртуализации, реализованного в системе оркестрации, находится на уровне программных продуктов лидеров рынка (ближайшим аналогом является vCenter разработки компании VMware).

2.2.6 Модуль управления удаленными рабочими столами

Модуль управления удаленными рабочими столами (Virtual Desktop Infrastructure – VDI) предназначен для создания защищенных пользовательских сред на базе виртуальных рабочих столов Windows и Linux, а также с применением опубликованных приложений Windows и Linux. VDI-брокер обеспечивает следующие основные функции:

- Автоматическое развертывание ВМ с удаленными рабочими столами на платформе виртуализации,
- Аутентификация пользователей по внешним базам (Microsoft Active Directory, Open LDAP, FreeIPA и многие другие),
- Управление сессиями доступа к удаленным рабочим столам и опубликованным приложениям.

Разработан защищенный протокол доступа к удаленному рабочему столу на базе протокола SPICE. Разработанный протокол доступа предполагает использование таких кодеков, как H.264/H.265, и позволяет достичь превосходного качества видео, статических изображений, текста, аудио и т.д. при сравнительно низком использовании полосы пропускания (сопоставима с полосой, используемой протоколом PCoIP компании Teradici).

2.2.7 Резервное копирование и репликация

Модуль резервного копирования позволяет делать копии и восстанавливать ВМ на уровне образов виртуальных дисков. Также модуль резервного копирования позволяет реплицировать виртуальные диски ВМ между основной и удаленной площадкой, позволяя строить катастрофоустойчивые решения на базе ПК «Иридиум».

Модуль резервного копирования позволяет делать резервные копии ВМ в процессе их работы, при этом консистентность данных на виртуальных дисках обеспечивается следующими двумя способами:

- Посредством агентского ПО, установленного в гостевую ОС, выполняется сброс данных из кэшей виртуальных контроллеров ВМ на виртуальный диск, после чего создается снимок состояния ВМ, и происходит резервное копирование «замороженного» базового виртуального диска ВМ. По окончании резервного копирования происходит консолидация снапшота с базовым диском.
- Посредством создания слепка виртуальной памяти ВМ (вместе со всеми данными в кешах виртуальных контроллеров), после чего также создается снимок состояния ВМ, и происходит резервное копирование «замороженного» базового виртуального диска ВМ. При восстановлении ВМ виртуальная память восстанавливается из ранее сделанного слепка памяти.

2.2.8 Межсетевой экран

Модуль межсетевого экрана (МСЭ) предназначен для защиты виртуальных сетей с подключенными к ним ВМ. Он является сертифицированным МСЭ, а также сертифицированным средством криптозащиты информации (СКЗИ), обеспечивающим шифрование наложенных туннелей с использованием криптоалгоритмов ГОСТ.

- Максимальная скорость фильтрации до 50 Гбит/сек
- Фильтрация как на третьем уровне (маршрутизируемый режим), так и на втором уровне (режим коммутации или «прозрачный» МСЭ)
- Фильтрация по любым полям в заголовке сетевого пакета (вплоть до седьмого уровня)
- Фильтрация по расписанию
- Фильтрация по доменному имени
- Система обнаружения вторжений (СОВ), работает как в активном, так и пассивном режиме

2.2.9 Мониторинг

Модуль мониторинга обеспечивает отслеживание статуса всех компонент платформы виртуализации (хосты, виртуальные машины, хранилища), выявление неисправностей, сбор логов и прочей телеметрии, анализ информации, отображение ее в графическом виде и т.д. Ближайший аналог – продукт VMware Aria Operations.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

	Номера листов (страниц)				*Всего листов (страниц) в докум.*	*№ документа*	*Входящий номер доп. Документа и дата*	*Подп.*	*Дата*
Изм.	*изменен-ных*	*заменен-ных*	*новых*	*аннулиро-ванных*					