Astra
Infrastructure
Cloud

Astra Infrastructure Cloud. Руководство по проектированию.

1 Введение

Документ содержит:

- обзор дизайна и архитектуры Облачной Платформы «Astra Infrastructure Cloud» на базе продуктов «Группы Астра» и решений по Информационной Безопасности от сторонних производителей;
- описание компонентов решения, зависимостей и связей;
- требования к программно-аппаратной платформе для развёртывания решения.

Документ предназначен для:

- экспертов со стороны заказчика, задействованных в рассмотрении предлагаемой функциональности, утверждении проектной архитектуры, планов и требований;
- специалистов, задействованных в развёртывании решения;
- руководителей, отвечающих за оценку функциональности и перспектив дальнейших разработок.

Astra Infrastructure Cloud является сложным программным продуктом, состоящим из большого количества компонент, и требует тщательного проектирования для корректной работы.

2 Краткое описание платформы

Облачная платформа (ОП) «Astra Infrastructure Cloud» (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».

Для обеспечения требований Информационной Безопасности системы на различных уровнях предполагается использовать продукты сторонних производителей. В данном документе приведено решение, использующее следующие компоненты:
- межсетевой экран;
- антивирусное ПО;
- системы управления событиями информационной безопасности.

2.1 Базовая и Стандартная редакции платформы AIC

ПО AIC поставляется в двух редакциях: Базовая (Starter) и Стандартная (Pre-Cloud)[1].

Базовая редакция включает минимально необходимый набор компонент 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).

Стандартная Редакция включает все компоненты Базовой Редакции, и дополнительные компоненты:

- ПО «Astra Automation»;
- ПО «Astra Monitoring»;
- ПО «DCImanager»;
- ПО «BILLmanager».

Возможности Базовой и Стандартной редакций по работе с инфраструктурными сервисами, такими как программно-определяемые - сети (SDN), хранилища (SDS), а также по базовым показателям надёжности и доступности не различаются.

Табл.1. Различия в базовой и стандартной редакциях

	Базовая редакция	Стандартная редакция
ОС СН «Astra Linux SE»	+	+
ПК СВ «Брест»	+	+
ПК службы каталогов «ALD Pro»	+	+
СРК «RuBackup»	+	+
ПО «DCImanager»	±	+
ПО «Astra Monitoring»	±	+
ПО «Astra Automation»	—	+
ПО «BILLmanager»	—	+

2.2 Ограничения

В этом документе приводится описание платформы, не учитывающее все возможные сценарии и требования к масштабируемости, производительности, отказо- и катастрофо- устойчивости, информационной безопасности, предъявляемые к конечному решению. Окончательные характеристики и конфигурации программных и аппаратных средств могут быть скорректированы исходя из функциональных и нефункциональных требований, технического задания, по итогам проведения нагрузочного тестирования и опытной эксплуатации платформы в рамках пилотных проектов конечного целевого решения, или иных нормативных документов.

[1] Маркетинговые названия могут отличаться

3 Требования к инфраструктуре

Для развёртывания компонентов решения необходимо обеспечить готовность инфраструктуры на стороне Заказчика. В разделах этого документа, описывающих отдельные компоненты решения, приводятся характеристики рекомендуемого аппаратного обеспечения, коммутации сети и настройки системы хранения данных. Предполагается, что все аппаратные компоненты инфраструктуры имеют минимальное территориальное распределение, используют выделенные каналы связи и обеспечивают требуемые параметры и характеристики надёжности и производительности.

3.1 Требования к операционной системе

Для установки ОП AIC требуется ОС Astra Linux SE в редакции «Смоленск» или «Воронеж».
Необходимо соблюдать идентичность версий ОС на всех серверах ОП.
Для установки ОС не требуется подключения к сети Интернет.

3.2 Требования к системе разрешения имён

Для корректной работы AIC, компонентам облачной платформы должен быть доступен сервер системы доменных имён (DNS - Domain Name System).
Все компоненты облачной платформы должны иметь полностью уточнённое доменное имя (FQDN - Fully Qualified Domain Name).
Рекомендуется использования основного доменного имени вида **aic**.sld.tld, где sld.tld – домен, используемый у заказчика.
Для серверов ALD Pro не рекомендуется использовать доменные имена первого уровня. Это значит, что нежелательно использовать имена, состоящие из одного слова, например domain, testdomain, mydomian. Следует использовать имена уровня два и более.

Все имена компонент ОП AIC должны иметь соответствующие записи в используемом DNS сервере. Требуется обеспечить как прямую, так и обратную трансляцию.

Табл.2. Пример описания соответствий IP адресов и FQND.

FQDN узла	VLAN	IP адрес	Описание
front.aic.customer.ru	300	192.168.1.100	Имя узла ПК СВ «Брест» с ролью Front
brestnode1.aic.custumer.ru	100	192.168.2.101	Первый узел кластера
brestnode2.aic.custumer.ru	100	192.168.2.102	Второй узел кластера
brestnode3.aic.custumer.ru	100	192.168.2.103	Третий узел кластера
dc1.aic.custumer.ru	101	192.168.7.80	Первый DC ALD Pro
dc2.aic.custumer.ru	101	192.168.7.81	Второй DC ALD Pro
rba1.aic.customer.ru	110	192.168.9.10	Первичный сервер RuBackup
rba2.aic.customer.ru	110	192.168.9.11	Медиа-сервер RuBackup
bootstrap.aic.customer.ru	100	192.168.2.2	bootstap сервер

3.3 Требования к сертификатам

Доступ к управляющим интерфейсам ОП AIC осуществляется через протокол HTTPS, обеспечивающий шифрование данных. Процесс шифрования требует создания сертификатов. Сертификат должен быть выдан уполномоченным центром сертификации и включать в себя полный набор сертификатов от центров сертификации, которые его выдали. Возможно использование как публичных, так и приватных центров сертификации.

В случае отсутствия доступа к внешним центрам сертификации, возможно использование центра сертификации на основе ПО «DogTag» входящего в состав ОС СН ALSE или программных продуктов третьих производителей.

Центр сертификации DogTag представляет собой систему управления сертификатами корпоративного класса, обеспечивающую управление полным жизненным циклов сертификатов. Под термином "сертификат" подразумевается сертификат публичного (открытого) ключа, использующий цифровую подпись центра сертификации для аутентификации (удостоверяющий сертификат). Сертификаты являются текстовыми файлами и могут содержать такую информацию, как имена лиц или названия организаций, адреса и т.д. Сертификаты используются для того, чтобы удостовериться в принадлежности открытого ключа субъекту. Центр сертификации DogTag поддерживает следующие возможности работы с сертификатами:

- Выпуск сертификатов;
- Выдачу (публикацию) сертификатов;
- Отзыв сертификатов;
- Создание и публикацию списков отзыва сертификатов;
- Профили сертификатов;
- Протокол публикации сертификатов Simple Certificate Enrollment Protocol (SCEP);
- Создание локального удостоверяющего центра (Registration Authority, LRA) организации аутентификации и управлениям политиками;
- Сохранение и восстановление закрытых ключей;
- Управление токенами (представляют собой объекты, которые обеспечивают управление ключами и сертификатами);
- Профили токенов;
- Выдачу, блокировку, восстановление и очистку токенов;
- Запись токенов.

Порядок установки и настройки центра сертификации DogTag описан в документации ОС СН Astra Linux.

3.4 Доступ к базовым сетевым службам

Для корректной работы ОП AIC требуется обеспечить доступ к следующим сетевым службам и сервисам:

- NTP (Network Time Protocol) – сервис точного времени
- DNS (Domain Name System) – система разрешения имён. Все имена, используемые в ОП, должны иметь соответствующие записи в используемом DNS сервере. Требуется обеспечить как прямую, так и обратную трансляцию.

- LDAP (Lightweight Directory Access Protocol) или AD (Active Directory) – служба каталогов.

ОП AIC предоставляет возможность использования собственных сетевых служб в виде виртуальных машин.
В случае LDAP/AD, внешняя, по отношению к ОП служба каталогов может быть использована на уровне установки доверительных отношений. Внутри ОП AIC, в качестве службы каталогов используется ПО ALD Pro.

Внимание! Для повышения доступности служб AIC рекомендуется вынесение по крайней мере одного КД ALD Pro за пределы Облачной Платформы

3.5 Требования к сетевому оборудованию

На каждом физическом узле (сервере) ОП должно быть установлено не менее 2-х двух-портовых 10ГБит Ethernet адаптеров, предназначенных для передачи управляющего трафика и трафика виртуальных машин.

В каждом сервере должен быть установлен BMC (Base Management Controller) контроллер с поддержкой технологии IPMI (Intelligent Platform Management Interface). Один Ethernet порт BMC контроллера должен быть доступен для подключения к выделенной сети управления. Пример реализации BMC для различных производителей серверного оборудования приведён в Табл.3.

Табл.3. Пример реализации BMC

Производитель	Технология на основе IPMI
Cisco	IMC – Integrated Management Controller
DELL	iDRAC – Integrated Dell Remote Access Card
HP	iLO – Integrated Lights-Out
IBM	IMM – Integrated Management Module
Lenovo	IMM – Integrated Management Module
Oracle	ILOM – Integrated Lights Out Manager
Supermicro	SIM – Supermicro Intelligent Management
Yadro	OpenBMC – Open Base Management Controller

Для обеспечения отказоустойчивости в системе применяется агрегация линков с использованием протокола LACP (Link Aggregation Control Protocol). При этом необходимо использовать 2 коммутатора, распределяя линки агрегатов между ними.

Рекомендуется выделить отдельный коммутатор для сетей IPMI. Достаточная скорость интерфейсов - 1 Гбит/с.

На отдельные коммутаторы рекомендуется вынести сети доступа к системам хранения данных (СХД) - Ceph External/Storage и Ceph Internal.

Количество портов используемых коммутаторов определяется доступностью оборудования и экономической целесообразностью. Разумно заложить портовую ёмкость с учётом планируемого развития ОП AIC.

При использовании внешних iSCSI (Internet Small Computer System Interface) хранилищ требуется установка дополнительных Ethernet адаптеров для сети передачи данных.
Рекомендуемое минимальное количество портов для подключения к iSCSI хранилищу – 2. Рекомендуемая минимальная скорость подключения – 10Гбит/с на порт.

При использовании программно-определяемой СХД, такой как Ceph, требуется установка дополнительных Ethernet адаптеров для сети передачи данных.
Рекомендуемое минимальное количество портов для подключения к хранилищу – 2. Рекомендуемая минимальная скорость подключения – 10Гбит/с на порт. Для высоконагруженных систем рекомендуемая скорость подключения - 40Гбит/с.

При высоких требованиях к производительности СХД может потребоваться оборудование более высокого класса производительности.
Внимание! Не допускается передача данных сети хранения (iSCSI, Ceph и пр.) по сетевым интерфейсам, используемым для передачи управляющего трафика и трафика виртуальных машин.

Все подключения, кроме подключения в BMC выполняются с использованием 2-х интерфейсов в режиме bonding. Для повышения производительности и отказоустойчивости необходимо использование протокола LACP. Интерфейсы должны быть подключены попарно к отдельным коммутаторам.

Со стороны сетевого оборудования требуется поддержка следующих протоколов и технологий:

- 802.1q (VLAN - Virtual Local Area Network) - используется для создания логических сетей внутри физической сети. Позволяет разделить большую сеть на несколько небольших, каждая из которых может быть настроена для определённых приложений или сервисов. Это позволяет эффективно управлять трафиком и обеспечивать безопасность данных;
- VXLAN (Virtual eXtensible Local-Area Network) - технология инкапсуляции исходных Ethernet кадров в IP/UDP пакеты. Используется для создания логических сетей поверх существующей высокоскоростной IP сети ЦОД либо нескольких ЦОД с целью обеспечения сетевой связности конечных сетевых устройств на втором уровне модели OSI. VXLAN позволяет создать до 16 миллионов логических сетевых сегментов по сравнению с технологией 802.1q (VLAN), где количество сегментов не может превышать 4096. Может потребоваться при развёртывании ОП AIC в режиме федерации или в случае необходимости построения комплексной сети;
- VRRP (Virtual Router Redundancy Protocol) - используется для обеспечения отказоустойчивости и высокой доступности в сетях. Он позволяет создать виртуальный маршрутизатор, который объединяет несколько физических маршрутизаторов в единую систему. Если один из физических маршрутизаторов выходит из строя, VRRP автоматически переключает трафик на другой маршрутизатор, обеспечивая непрерывность работы сети. Протокол VRRP также позволяет управлять конфигурацией маршрутизаторов и обновлять их в режиме реального времени. Поддержка VRRP может потребоваться при разворачивании сервисов в высокодоступной (HA – High Available) конфигурации;
- BGP (Border Gateway Protocol) - используется при создании ОП состоящей из нескольких зон доступности (availability zone). Позволяет обеспечить эффективное распределение

трафика между различными облачными ресурсами и дата-центрами. Также используется для обеспечения высокой доступности и отказоустойчивости облачной инфраструктуры. Например, если один из дата-центров выходит из строя, BGP автоматически перенаправляет трафик на другие доступные дата-центры, что позволяет минимизировать время простоя и обеспечить непрерывность работы приложений;

- MP-BGP (многопротокольный BGP) - протокол динамической маршрутизации с поддержкой EVPN адресации, используемой в VXLAN сетях для распространения маршрутной информации. Также используется для обеспечения высокой доступности и отказоустойчивости сети облачной инфраструктуры за счет анонса и получения маршрутной информации по нескольким линиям связи и возможности автоматического переключения маршрутов в случае сбоев. Например, если один из дата-центров выходит из строя, BGP автоматически перенаправляет трафик на другие доступные дата-центры, что позволяет минимизировать время простоя и обеспечить непрерывность работы приложений;
- STP (Spanning Tree Protocol) – используется для приведения сети Ethernet с множественными связями к древовидной топологии. Происходит это путём автоматического блокирования ненужных в конкретный момент времени для полной связности портов. Если в сети используется STP, сетевое оборудование должно поддерживать этот протокол для предотвращения петель в топологии;
- LACP (Link Aggregation Control Protocol) - используется для агрегации сетевых интерфейсов (портов) сетевое оборудование должно поддерживать LACP;
- QoS (Quality of Service) - Если важна приоритетность трафика, сетевое оборудование должно поддерживать QoS-механизмы для управления пропускной способностью и задержкой;
- VRF - технология, позволяющая на базе одного физического маршрутизатора создать несколько виртуальных. У каждого виртуального маршрутизатора можно определить свой набор сетевых интерфейсов, таблицу маршрутизации и прочие параметры. Используется для логического и административного разделения сетей на третьем уровне модели OSI;
- PIM - семейство протоколов, используемых для построения маршрутизации многоадресных (мультикаст) IP пакетов. Используется в сетях VXLAN для распространения broadcast, unknown-unicast и multicast трафика);
- OSPF (Open Shortest Path First) или IS-IS - протоколы динамической маршрутизации, используемые для распространения маршрутной информации и нахождения кратчайшего либо наиболее приоритетного пути прохождения IP пакетов от источника до назначения.

Вопрос организации сети выходит за рамки этого документа и требует отдельного проектирования.

3.6 Порты и протоколы необходимые для работы подсистем AIC

Для корректного взаимодействия компонент ОП AIC между ними должна быть настроена сетевая связанность. На узлах и межсетевых экранах должны быть открыты порты, список которых приведён в Приложении 1.

Проверить доступность портов можно с помощью различных утилит ОС Linux.

```
#Пример проверки открытых портов для контроллера домена с использованием nmap:
#проверка TCP портов
sudo nmap -sT -p 80,443,389,636,88,464,53,135,139,445,4505,4506,10050,22,8000,8008,30000,749,5001 {ip-адрес контроллера домена}
#проверка UDP портов
sudo nmap -sU -p 53,88,123,137,138,464 {ip-адрес контроллера домена}
```

3.7 Требования к серверному оборудованию

В ОП AIC выделяются следующие основные роли серверов:

- Сервер Контроля Облачных Ресурсов (СКОР) – несёт на себе все функции управления ОП и является частью Блока Контроля Облачных Ресурсов (бКОР)
- Сервер Блока Клиентских Ресурсов (СБКР) – используется для размещения пользовательской нагрузки в виде виртуальных машин и PaaS сервисов.

Минимальное количество СКОР – 3 (три) единицы. При необходимости возможно увеличение количества СКОР инкрементами по 2N+1.
В каждом СКОР должно быть не менее 32-х физических ядер и 128 ГБ RAM, 4х25ГБит или 4х10ГБит Ethernet (LACP), 1х1ГБит BMC, 2х500 ГБ SSD/NVME. При использовании системы SDS необходимо использование дополнительных Ethernet контроллеров.

Минимальное количество СБКР – 2 (две) единицы. При необходимости возможно увеличение количества СБКР инкрементами по 1. Количество СБРК зависит от количества виртуальных машин с пользовательской нагрузкой, нагрузки на CPU и RAM и других критериев.

В каждом СБКР рекомендуется наличие не менее 16-х физических ядер и 64 ГБ RAM, 4х25ГБит или 4х10ГБит Ethernet (LACP), 1х1ГБит BMC, 2х500 ГБ SSD/NVME.

Требования к минимальному количеству ресурсов для тестовой среды приведены в разделе 7.8.

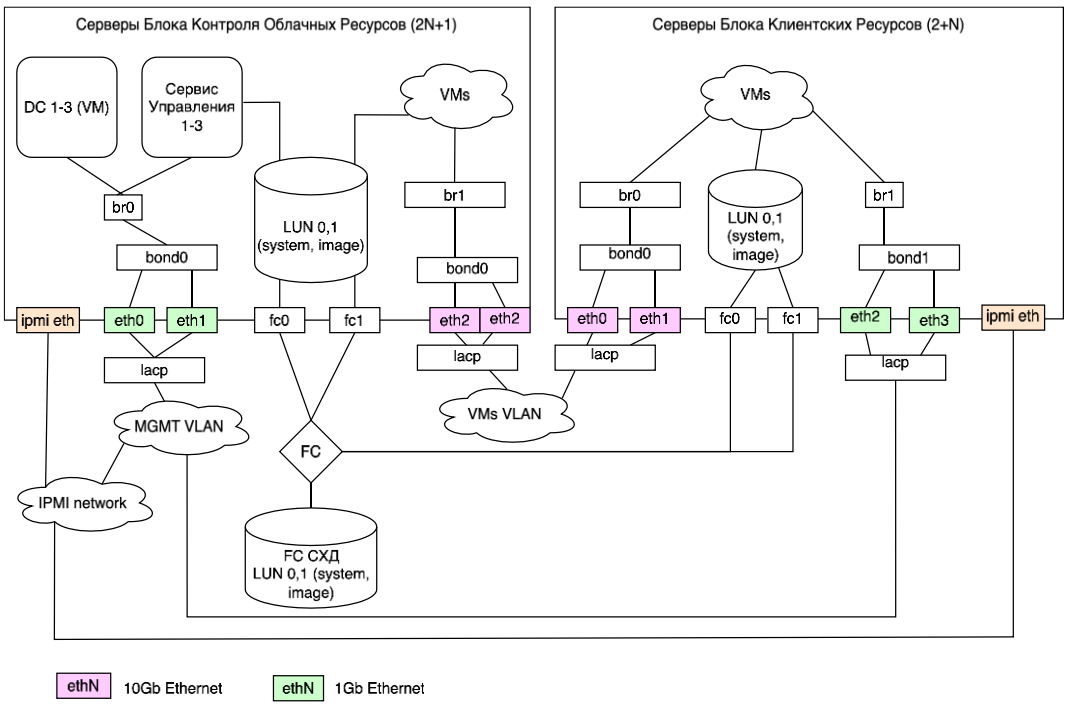


Рис.1. Пример подключения серверов AIC к сетям Ethernet и Fibre Channel.

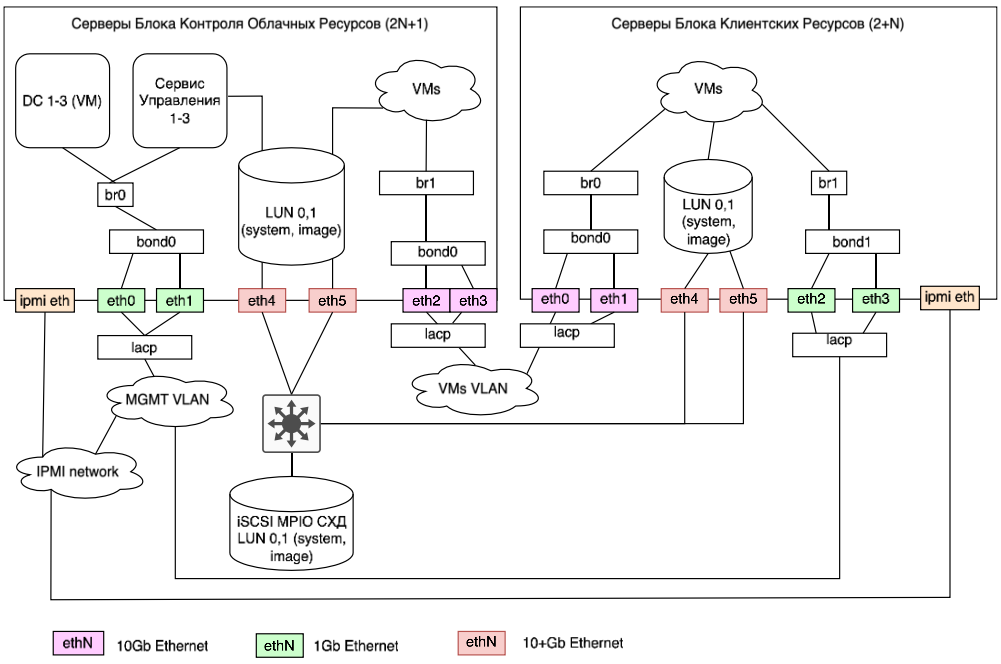


Рис.2. Пример подключения серверов AIC к сетям Ethernet и iSCSI MPIO СХД.

4 Архитектура облачной платформы AIC

4.1 Общая схема и основные компоненты

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

Облачная платформа включает в себя набор продуктов ГК Астра (см. Рисунок «Используемые компоненты решения на основе ОП AIC»):

- ОС СН «Astra Linux SE» (ALSE);
- ПК управления службами каталогов «ALD Pro»;
- ПК СВ «Брест»;
- SDS «Ceph» (опционально);
- Система резервного копирования «RuBackup».

Голубым цветом на Рис.3 представлен минимальный набор компонент решения. Белым цветом показаны компоненты, предлагаемые к интеграции для достижения оптимальной функциональности. Красным цветом обозначены примеры компонент сторонних поставщиков.

Рис.3. Используемые компоненты решения на основе ОП AIC

Облачная платформа представляет собой единый набор масштабируемых взаимосвязанных программных и инфраструктурных блоков, что позволяет создать решение, соответствующее практически любым потребностям Заказчика.

Программные и инфраструктурные составляющие решения могут быть объединены в блоки, роли и сервисы, состоящие, в свою очередь, из набора ПО, решающего определённый список задач. Так Блок Контроля Облачных Ресурсов включает все элементы ОП AIC предназначенные для управления ОП, а роль (функция) и сервис управления ссылаются на ключевые программные продукты ОП – «ALD Pro», ПК СВ «Брест» и «DCImanager». Детальная информация

представлена в разделе «Блоки составляющие ОП AIC».

Табл.4. Основные программные блоки, роли, сервисы и компоненты. Зелёным цветом выделены базовые компоненты являющиеся частью решения[2].

Блок	Роль (Функция)	Сервис	Компоненты
Блок Контроля Облачных Ресурсов (бКОР)	Сервисы Роли Установки и Восстановления	Сервер загрузки и обслуживания	o-day AIC Operations Console (VM) Management Console
	Сервисы Роли Управления	Сервис Управления	ALD Pro
			Брест
			DCImanager
		Сервис Web Консоли	Брест
			Bill Manager
			DCImanager
			ALD Pro
		Портал самообслуживания	BillManager
			Брест
	Сервисы Роли Сопровождения	Сервис Автоматизации	Astra Automation
		Сервис Защиты Данных	RuBackup
		Сервис Отчётности	Astra Monitoring
			BILLmanager
	Контроль Облачных Сервисов	Containers	
		PaaS	
		SaaS	
	Контроль Облачных Данных	Сервис Программно-определяемых СХД	Minio
			Ceph
		Сервис Защиты и Восстановления Данных	RuBackup
Блок Клиентских Ресурсов (БКР)	Роль Управления Сервисами	KVM	Сервис Разработки
			Сервис Контейнеризации K8s
		VDI	VDI (СВРМ - Сервис Виртуализации Рабочих Мест)
	Сервис Защиты Данных Клиентов	RuBackup	

Сервисы и компоненты не входящие в текущую версию платформы:

- Сервис разработки и среды исполнения (GitFlic, Axiom JDK)
- Сервис оркестрации и контейнеризации (Nodus на базе Kubernetes/Docker)
- Сервис виртуализации рабочих мест (Termidesk)
- Сервис формирования отчётности (BI)
- Сервис управления данными пользователей (PostgreSQL)
- Сервисы класса SaaS

Состав ролей, сервисов и компонент может увеличиваться по мере развития ОП. Детальное описание ролей, сервисов и компонент описано в разделе «Блоки составляющие AIC».

[2] Зависит от вида поставляемой ОП AIC

Пользователи ОП AIC могут самостоятельно разрабатывать и внедрять роли (функции) и сервисы в ОП. Например, в Блоке Клиентских Ресурсов, для роли (функции) «Защиты Данных Клиентов» пользователи могут использовать СРК стороннего производителя.

4.1.1 Основные компоненты

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. Возможно установление двухсторонних доверительных отношений с существующей службой каталогов MS AD.

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)

Рис.4 и Рис.5 иллюстрируют пример общей схемы компонентов и связей.

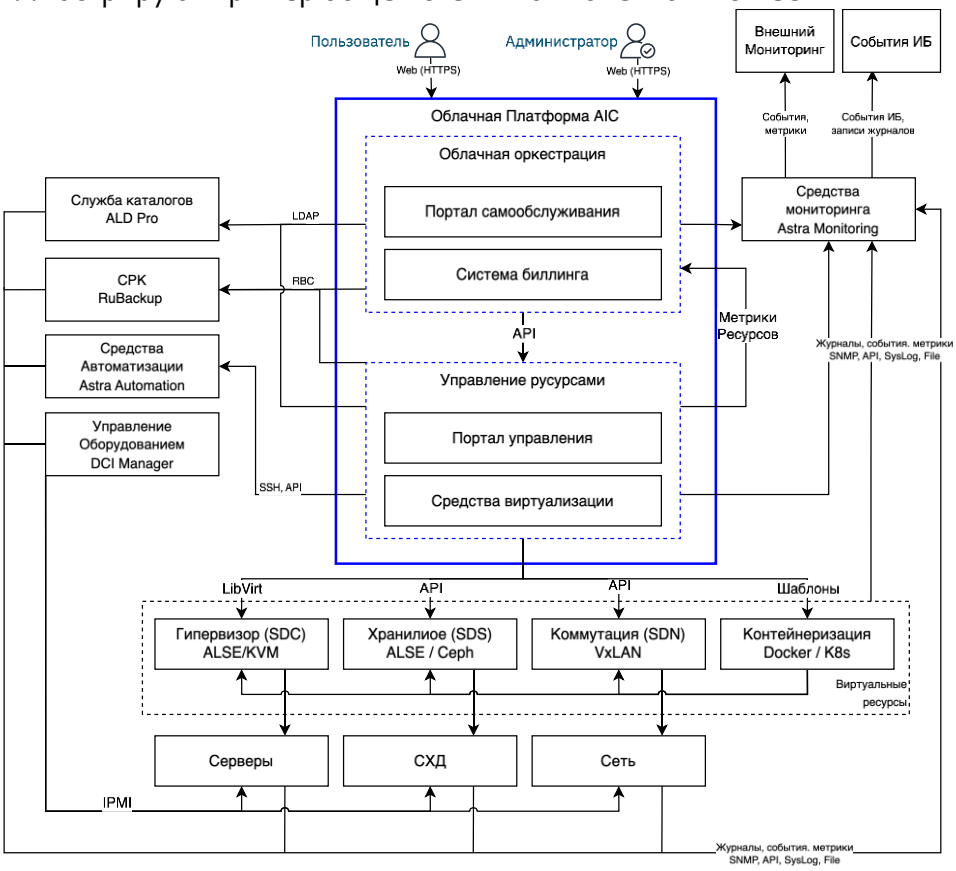


Рис.4. Логическая схема решения

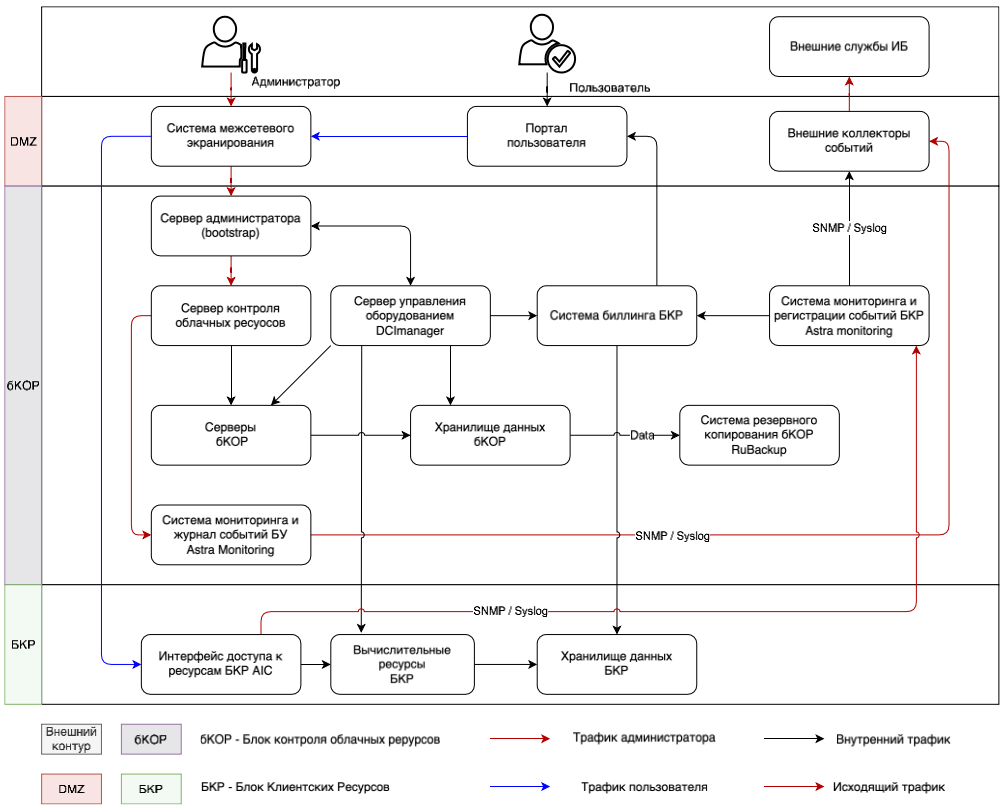


Рис.5. Диаграмма связей и зоны взаимодействия подсистем платформы

Табл.5. Функциональные модули

Элемент схемы	Краткое описание
Внешние службы ИБ	Возможное решение управления информацией и событиями безопасности (SIEM) на стороне Заказчика
Администраторы	Администраторы, осуществляющие поддержку функционирования всех компонентов внутри платформы
Пользователи	Пользователи Заказчика
Портал пользователя	Доступ к выделенным ресурсам Заказчика через пользовательский интерфейс на базе BILLmanager
Внешние коллекторы событий	Коллектор и обработчик событий мониторинга, поступающие со стороны виртуальных машин Заказчика
Система мониторинга и журнал событий	Модуль на базе решения Astra Monitoring
Блок Контроля Облачных Ресурсов	Далее бКОР, представляет собой блок из модулей управления платформой на базе KVM (Kernel-based Virtual Machine)
Блок Клиентских Ресурсов	Далее БКР, представляет собой блок из модулей управления клиентскими ресурсами на базе решения ПК СВ "Брест"
Сервер контроля Блока Клиентских Ресурсов (БКР)	Представляет собой фронтальные серверы, обеспечивающие доступ и управление ресурсами БКР
Сервер администратора (bootstrap)	Сервер для администраторов платформы, используемый на этапе внедрения ОП AIC, и обеспечивающий доступ к серверам управления виртуализацией

Элемент схемы	Краткое описание
Сервер контроля бКОР	Представляет собой центральный сервер управления ресурсами бКОР
Хранилище данных	Далее СХД, представляет собой аппаратную или программно-определяемую СХД как для бКОР, так и для БКР в виде отдельного модуля.
Вычислительные ресурсы	Используются для размещения виртуальных машин, на базе гипервизора KVM
Сервер управления оборудованием	Централизованная платформа (панель) управления, контроля состояния и диагностики серверного и сетевого оборудования на базе ПО DCImanager
Система резервного копирования бКОР	Система резервного копирования, обеспечивающая резервное копирование конфигурационных файлов и виртуальных машин бКОР, построенная с использованием ПО RuBackup

4.1.2 Блоки составляющие AIC

4.1.2.1 Блок Контроля Облачных Ресурсов

Блок Контроля Облачных Ресурсов (бКОР) предоставляет вычислительные мощности и хранилища для компонентов управления облачной инфраструктурой, а также обеспечивает функции оперативного управления, включая, но не ограничиваясь:

- предоставление информации о состоянии ключевых элементов платформы;
- сбор метрик и системных журналов (log-файлов);
- предоставление шаблонов ресурсов;
- накопление статистики использования, квоты, состояние используемых ресурсов;
- административный доступ, аутентификация и авторизация для административного персонала и пользователей.

ПК СВ «Брест» является ключевым компонентом ОП AIC, обеспечивает оркестрацию VM и управление вычислительными ресурсами, а также предоставляет возможности, среди которых:

Табл.6. Возможности ПК СВ «Брест»

HA	Обеспечение отказоустойчивости работы инфраструктуры и(или) сервисов
ACL, VDC, Multi-tenant	Гранулярное разграничение доступа между участниками одной инфраструктуры и участниками разных инфраструктур
DRS	Гибкое планирование вычислительных ресурсов и ресурсов хранения/сетевых коммуникаций между инфраструктурами
Security Groups	Контроль над сетевыми взаимодействиями между инфраструктурами и глобальной сетью
Market Place	Унификация и ограничение набора используемых ОС и их версий в пользовательских инфраструктурах/сервисах
GUI Views	Представление различных наборов окружений (пример: портал самообслуживания) в веб-оболочке
GUI View Restrictions	Изменение отображаемых функций в различных наборах окружений (пример: портал самообслуживания, портал администраторов) в веб-оболочке
ShowBackCost	Тарификация использования ресурсов и расчёт стоимости + выставление счета для конечного потребителя с помощью внешних биллинговых систем (BILLmanager)
Federation	Управление географически-распределёнными площадками из единого веб-портала

Overcommitment	Возможность осуществления выделения определённого объёма физических ресурсов серверного оборудования одновременно нескольким клиентам
IaC	Контроль над инфраструктурой и интеграция с другими системами с точки зрения автоматизированного подхода, инфраструктура как код (Terraform, API)
Backup	Выполнение резервного копирования ВМ
Contextualiztion	Автоматизированное конфигурирование параметров ВМ согласно каким-либо требованиям Администратора
Cloning	Возможность создания копий образов на базе ВМ
VM Groups (Affinity/Anti-Affinity)	Гибкое управление размещением различных ВМ относительно друг друга и по гипервизорам
VM Live-Migration / VM storage Live Migration	Миграция ВМ между гипервизорами и между хранилищами одного типа в живом режиме
VM Live Resizing	Изменение ресурсов ВМ в живом режиме
PCI/USB redirection	Перенаправление физических устройств с хоста внутрь ВМ (USB, GPU, NIC, RAID-controller[3])
Load-Balancing	Распределение нагрузки в виде ВМ по нескольким гипервизорам
Host/Network/Storage dynamic precedence	Возможность настроить динамическое изменение выбора "оптимального" сервера виртуализации/сети/хранилища
SSO Kerberos	поддержка технологии единого входа на базе Kerberos
Domain Catalog Support	Поддержка служб каталогов ALD Pro / Freelpa / AD DS
VM GUI view	Подключение к ВМ из веб-интерфейса через соответствующий клиент по протоколам RDP (client), SPICE (web/client), VNC (web/client), RDP и SSH (web - только в сервисном режиме)
NUMA	Создание и редактирование представления NUMA (количество сокетов, ядер, потоков) внутри ВМ
QoS	шейпинг трафика и ограничение запросов ввода/вывода для дисковой подсистемы

бКОР так же содержит узел администрирования (в виде VM), который используется при первоначальной настройке платформы (bootstrap).

4.1.2.2 Блок клиентских ресурсов

Блок клиентских ресурсов (далее БКР) предоставляет вычислительную инфраструктуру для пользовательских виртуальных машин, хранения данных виртуальных машин и образов виртуальных машин, сервисов VDI, сервисов защиты данных (н-р RuBackup), а также сервисов PaaS и SaaS. Предполагается, что разворачивание сервисов в БКР, и их интеграция выполняется пользователями ОП AIC самостоятельно.

ОП AIC состоит из одного блока управления и одного или нескольких БКР.

4.1.3 Роли (функции) и сервисы в AIC

4.1.3.1 AIC Installation and Recovery Services (РУВ - сервисы Роли Установки и Восстановления)

Роль РУВ состоит из сервиса «Bootstrap & Service node» (СЗО - сервер загрузки и обслуживания) необходимого как на этапе установки ОП AIC, так и в дальнейшем ходе эксплуатации.

В процессе установки ОП AIC, в инфраструктуре заказчика разворачивается СЗО (в виде аппаратного сервера или VM) с набором ПО, необходимого для установки ОП. В набор ПО входит: PXE, DHCP, DNS серверы, набор инструментов Astra Automation, образы ОС, установочные образы компонент ОП, и т.д.

[3] опционально

В ходе эксплуатации, СЗО может использоваться для восстановления работоспособности ОП в случае сбоя, или для проведения работ регламентного обслуживания. При этом нет необходимости в постоянном функционировании СЗО. Аппаратный сервер или виртуальная машина могут быть выключены.

4.1.3.2 AIC Management Services (РУ - сервисы Роли Управления)

РУ состоит из сервисов: System Management (СУ - Сервис Управления), Web Consoles (СВК - Сервис Web Консоли) и Self-service portal (ПСО - портал самообслуживания).

Роль Управления описывает сервисы и компоненты являющиеся ядром ОП AIC и минимально необходимым набором ПО для функционирования ОП.

System Management (СУ - Сервис Управления) - состоит из набора связанного программного обеспечения: ПК СВ «Брест», служба каталогов ALD Pro и ПО управления инфраструктурными компонентами DCImanager[4].

Web Consoles (СВК - Сервис Веб Консоли) - предоставляет доступ через Web интерфейс к консолям управления продуктов ПК СВ «Брест», ALD Pro, DCImanager, BILLmanager[5].

Self-service portal (ПСО - сервис портала самообслуживания) - предоставляет доступ к порталу самообслуживания для пользователей ОП AIC. В редакции AIC 1.0 пользователю доступны Web консоль портала ПК СВ «Брест» (для Starter) или BILLManager (для Pre-Cloud)[6].

4.1.3.3 AIC Management Operation Services (РС - сервисы Роли Сопровождения)

Роль Сопровождения состоит из сервисов: Automation (СА - Сервис Автоматизации); Data Protection (СЗД - Сервис Защиты Данных); Monitoring, Billing (СО - Сервис Отчётности).

Сервис Автоматизации представляет собой ПО Astra Automation и позволяет автоматически устанавливать и управлять основными компонентами ОП AIC.

Сервис Защиты Данных - основан на ПО RuBackup и предназначен для создания резервных копий конфигураций ОП AIC, настроек компонент ОП, и резервирования виртуальных машин бКОР.

Сервис Отчётности построен на ПО Astra Monitoring и BILLmanager и предназначен для оценки состояния и производительности ОП AIC, создания отчётов, а также для оценки потребления ресурсов Облака пользователями.

4.1.3.4 Cloud Service Controller (КОС - Контроль Облачных Сервисов)

Роль КОС определяет инструменты и механизмы создания и управления PaaS и SaaS сервисами, а также сервисами, основанными на использовании контейнеров и микросервисной архитектуры.

---

[4] DCImanager не входит в базовую версию ОП AIC.

[5] BILLmanager не входит в базовую поставку ОП AIC

[6] В зависимости от редакции AIC.

4.1.3.5 Cloud Data Services (КОД - Контроль Облачных Данных)

Роль КОД определяет сервисы и компоненты необходимые для создания и управления программно-определяемыми СХД, а также управления резервным копированием и восстановлением данных в бКОР. Сервисы КОД могут быть использованы Блоком Клиентских Ресурсов для реализации сервиса СЗДК (Сервис Защиты Данных Клиентов).

4.1.3.6 Cloud Service Executor (РУС - Роль Управления Сервисами)

Роль Управления Сервисами БКР предназначена для создания и управления сервисами ОП AIC используемыми пользователями для создания виртуальных машин, сервисов VDI, кластеров Kubernetes, сред защищённой разработки и пр. Создание сервисов в РУС является задачей команды разработки заказчика.

4.1.3.7 Data Protection Services (СЗДК - Сервис Защиты Данных Клиентов)

Роль СЗДК БКР предназначена для описания сервисов и компонент используемых пользователями ОП для резервного копирования данных и виртуальных машин. В ОП AIC в качестве СРК предлагается использование ПО RuBackup. Однако, пользователи могут использовать любое ПО резервного копирования, совместимое с ОП AIC по программе Ready for Astra. Создание сервисов в СЗДК является задачей команды разработки заказчика.

4.1.4 Режим федерации

Возможно создание ОП состоящей из нескольких зон доступности (множество географически распределённых ЦОД) с управлением ресурсами из единого портала – режим Федерации.

Несколько экземпляров ПК СВ Брест, в составе бКОР, могут быть объединены в единый центр обработки и хранения данных (ЦОХД), который называется "федерация". В этом случае каждый экземпляр ПК СВ называется зоной. Один из экземпляров ПК СВ настраивается как ведущий, остальные – ведомые.

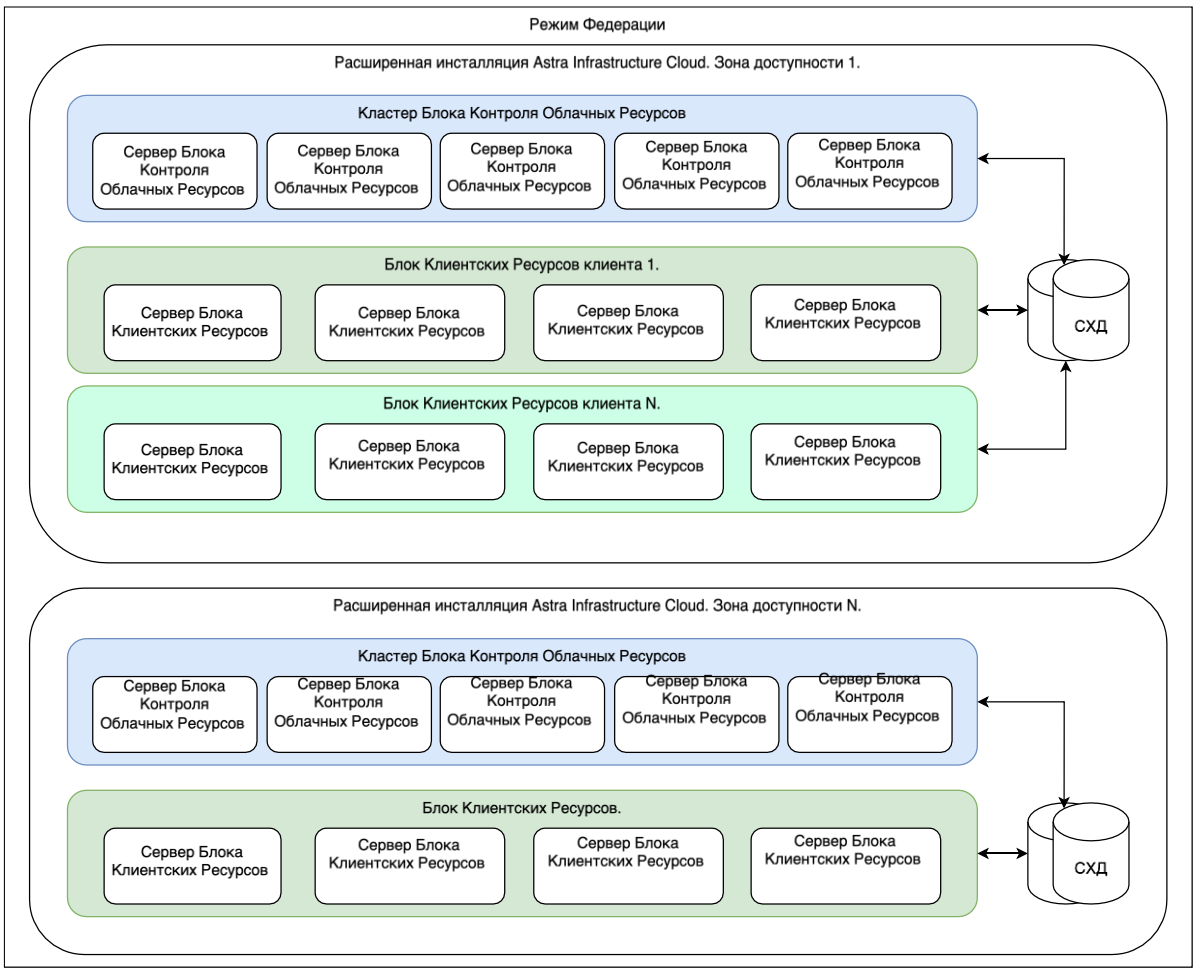


Рис.6. Режим федерации.

"Федерация" позволяет конечным пользователям использовать ресурсы, распределённые Администраторами единого ЦОХД, независимо от места их нахождения. Интеграция проходит комплексно, то есть пользователю, авторизованному в веб-интерфейсе определённой зоны, не придётся выходить из системы и вводить адрес другой зоны. веб-интерфейс ПК СВ позволяет изменять активную зону в любое время, а также автоматически перенаправляет запросы в ПК СВ в целевой зоне.

Служебный режим "федерация" является интеграцией с непосредственными связями. Все экземпляры ПК СВ имеют общую конфигурацию (общие таблицы БД) учётных записей пользователей, групп и полномочий. Доступ возможно ограничить до конкретных зон, а также до конкретных кластеров внутри данной зоны. Только ведущая зона ПК СВ имеет права на внесение записей в общие таблицы, у ведомых зон хранится локальная копия для чтения. Это гарантирует целостность данных без ущерба для скорости действий по считыванию.

Синхронизация выполняется путём настройки конфигурации ПК СВ для репликации только определённых таблиц. Репликация способна работать при соединениях на больших расстояниях и при нестабильных соединениях. В случае сбоя ведущей зоны и её длительной перезагрузки ведомые зоны могут продолжать работать в нормальном режиме, за исключением нескольких действий, например, создание нового пользователя или обновление паролей.

Новые ведомые зоны можно добавлять к существующей "федерации" в любой момент. Кроме того, администратор может добавить абсолютно новый экземпляр ПК СВ или импортировать

существующий в "федерацию", сохранив действующих пользователей, групп, конфигурацию и виртуальные ресурсы.

Перенос пользовательских виртуальных машин между зонами доступности не входит в штатный функционал ОП AIC, но может быть реализован с помощью ПО «RuBackup», или программных продуктов других производителей.

Установка ОП AIC в режиме «Федерация» требует тщательного планирования и предъявляет дополнительные требования к сетевому оборудованию и СЗИ.

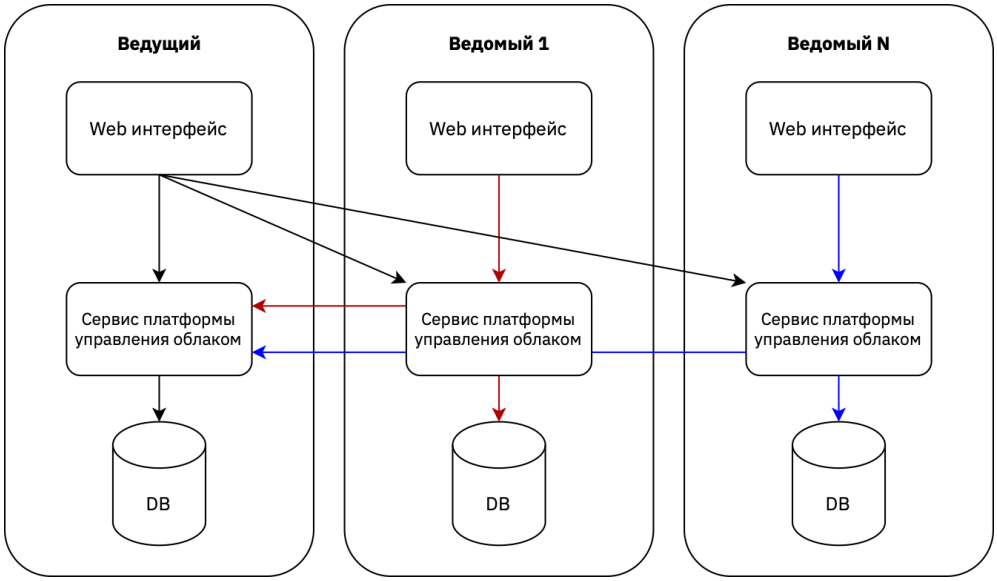


Рис.7. Управляющие потоки в режиме федерации.

4.1.5 Виртуальные машины и серверы в AIC

Компоненты ОП AIC находятся под управлением гипервизора KVM входящего в состав ОС СН ALSE.
В процессе установки AIC, первой устанавливаемой виртуальной машиной является bootstrap (сервер управления)[7]. С помощью bootstrap VM производится установка всех остальных компонентов AIC с помощью средств автоматизации Astra Automation. Bootstrap VM так же может выполнять роль репозитория пакетов необходимых для установки AIC в случае отсутствия подключения или ограничения доступа к внешним репозиториям ПО.

Каждый сервер, входящий в состав AIC, может быть назначен в Блок Контроля Облачных Ресурсов или в Блок Клиентских Ресурсов.

[7] Рекомендуется, при наличии аппаратных ресурсов, использовать выделенный bootstrap сервер.

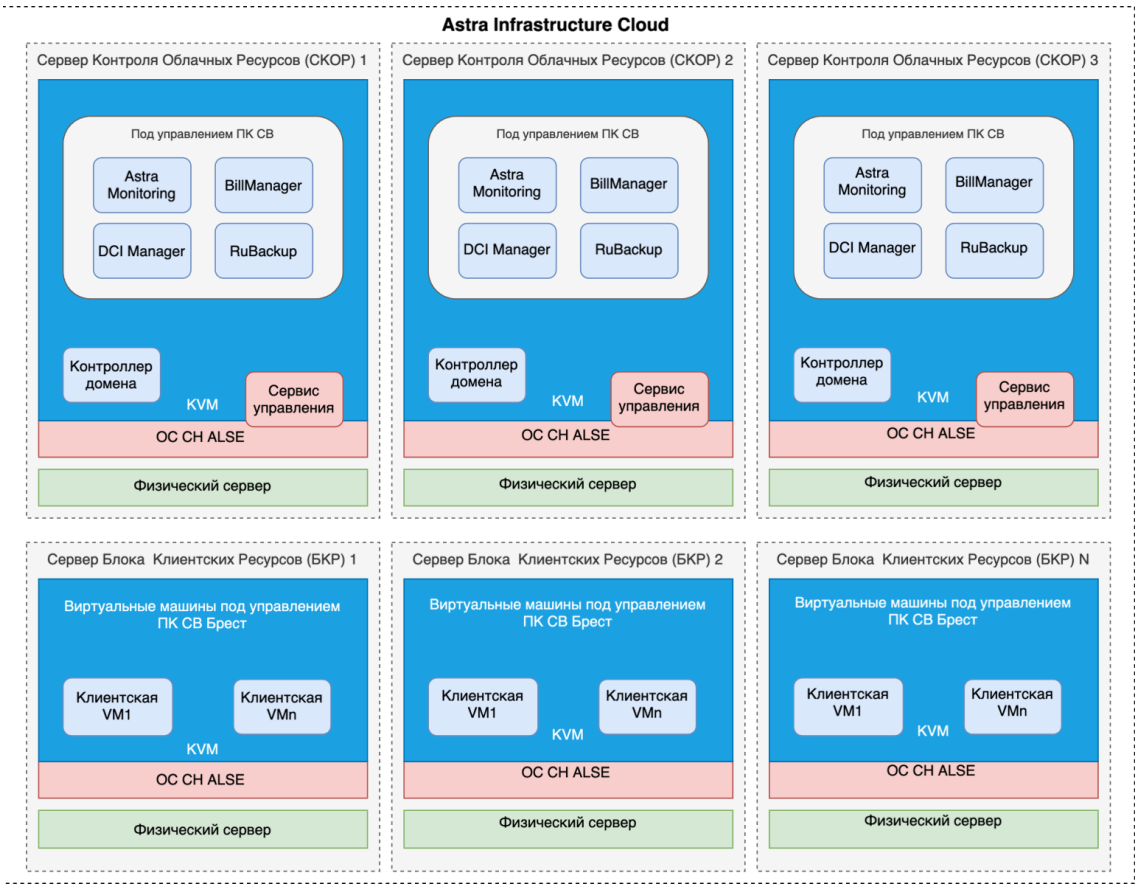


Рис.8. Виртуальные машины в AIC (вариант размещения)

В Блоке Контроля Облачных Ресурсов (бКОР) находятся основные и дополнительные сервисы AIC, среди которых[8]:

- Контроллер домена ALD Pro[9]
- СРК RuBackup
- Сервис Управления ПК СВ Брест (Front-End)
- DCImanager
- BILLmanager
- Astra Monitoring

Все компоненты бКОР находятся под управлением ПК СВ Брест.

Минимальное количество серверов бКОР – 3 ед.

В Блоке Клиентских Ресурсов (БКР) располагаются пользовательские виртуальные машины. Все виртуальные машины в БКР находятся под управлением бКОР.

На Рис.8 приведена конфигурация, в которой сервис ПК СВ «Брест» установлен в хостовую ОС, КД развёрнут в виде виртуальной машины. Так же, в виде виртуальной машины присутствует bootstrap сервер, который, после установки ОП AIC может быть выключен или удалён.

4.2 Архитектура сети

[8] Список сервисов в бКОР может меняться по мере совершенствования Astra Infrastructure Cloud

[9] Возможны различные варианты размещения КД. Подробнее в разделе «Рекомендации и варианты внедрения ОП AIC».

В AIC весь сетевой трафик разделён между несколькими обязательными VLAN.

- BMC – VLAN для IPMI трафика. Служит для управления физическими серверами со стороны платформы виртуализации ПК СВ Брест и ПО DCI Manager
- MGMT – управляющий VLAN. Предназначен для передачи управляющего трафика между компонентами AIC и управления виртуальными машинами.
- Backup – для передачи данных между компонентами AIC и СРК RuBackup
- iSCSI – для передачи данных между ОС СН ALSE и СХД по протоколу iSCSI.
- Ceph – для передачи данных между ОС СН ALSE и SDS Ceph
- VM – для трафика виртуальных машин

Разделение сетей обусловлено необходимостью деления потоков данных для обеспечения требований информационной безопасности, надёжности и производительности.
Количество VLAN в AIC может меняться в зависимости от набора компонент входящих в поставку AIC, требований ИБ и других условий использования ОП.

Количество IP адресов в каждой сети (netmask) необходимо выбирать исходя из планируемого роста количества служб, сервисов, зон доступности и других параметров.

Внимание! Совмещение трафика SDS Ceph и(или) iSCSI с другими данными категорически не рекомендуется и не является поддерживаемой конфигурацией.

На Рис.9 приведена схема деления трафика внутри AIC

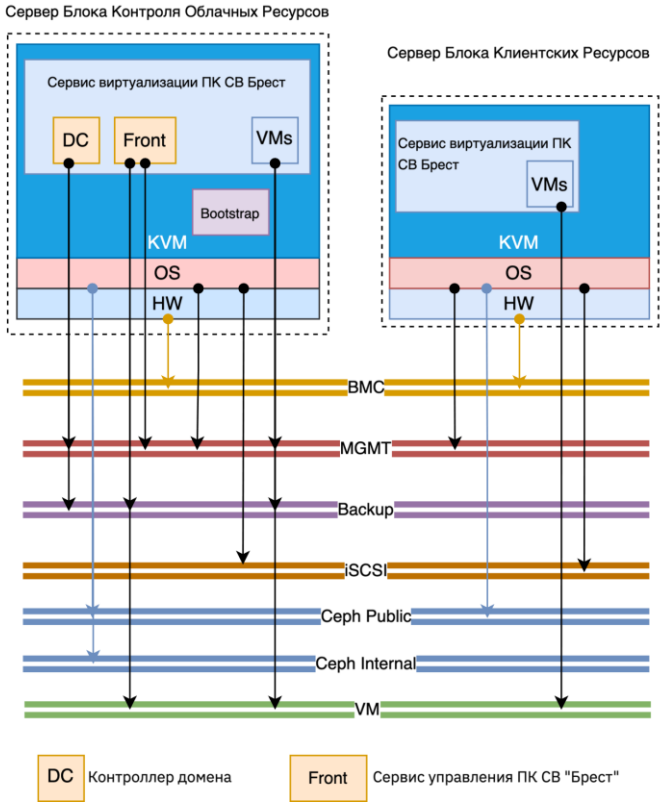


Рис.9. Деление IP трафика между VLAN

Табл.7. Стандартные VLAN в ОП AIC

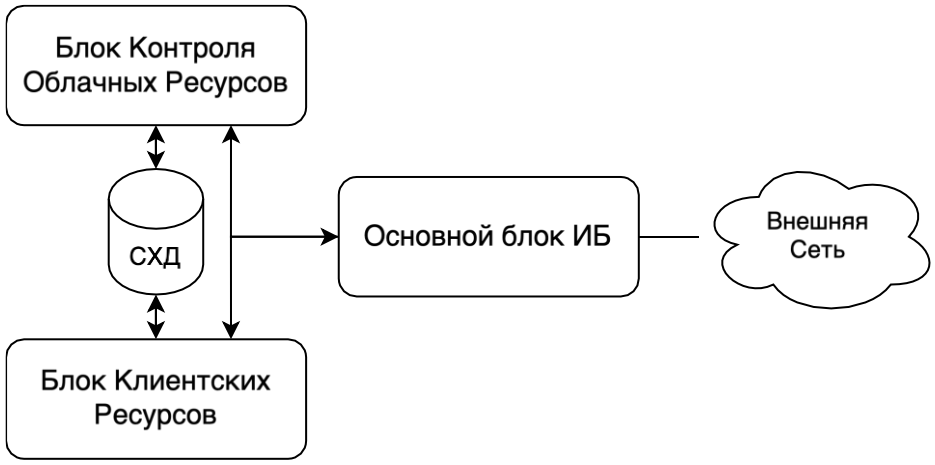
VLAN	Название	Описание
100	BMC	Объединяет BMC интерфейсы серверов для управления со стороны ПК СВ «Брест»

101	Management	Сеть для управляющего трафика
102	Backup	Сеть для создания резервных копий служебной информации AIC
103	iSCSI	Сеть передачи iSCSI трафика
104	Ceph Internal	Сеть для передачи служебного трафика SDS Ceph
104	Ceph Public	Сеть для передачи публичного трафика SDS Ceph
150	VM	Сеть трафика виртуальных машин

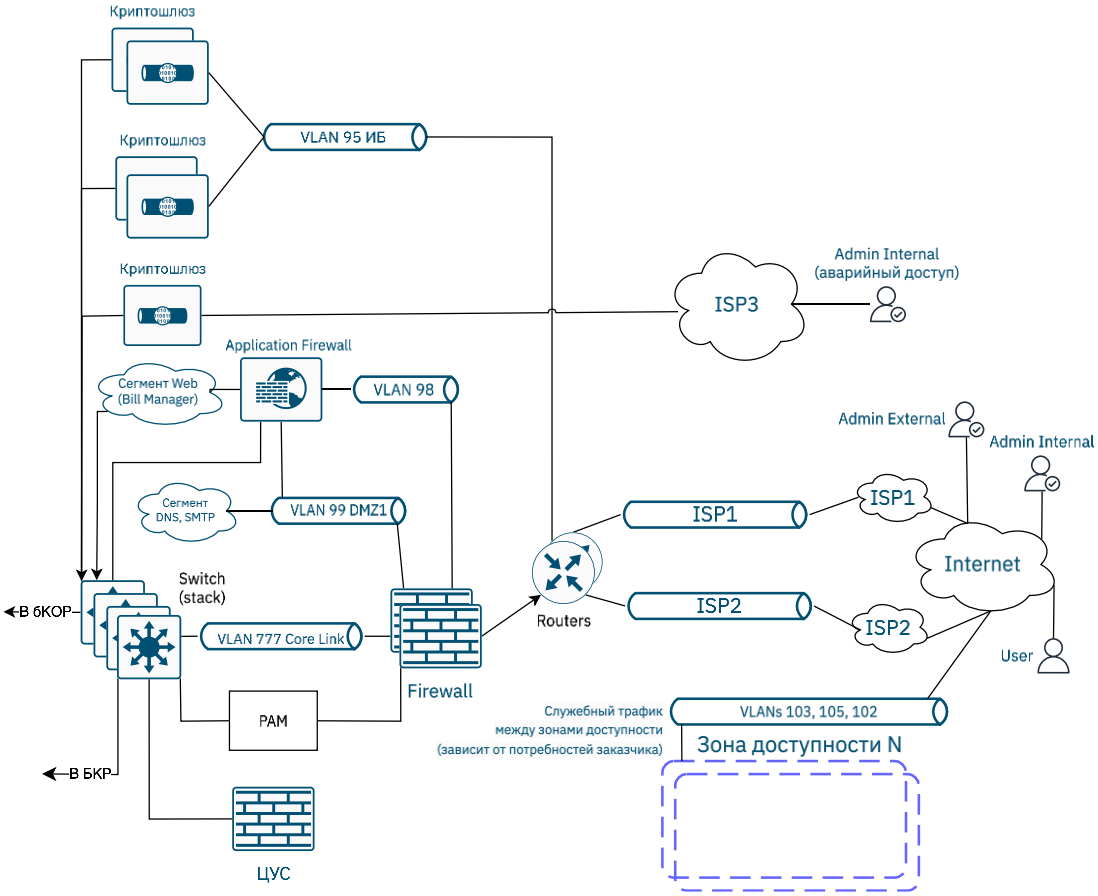
Облачная Платформа AIC допускает создание дополнительных VLAN в случае необходимости.

На Рис.10 «Комплексный пример сети» приведён пример сети в составе AIC

Общая схема



Основной контур ИБ


Криптошлюз
Криптошлюз
Криптошлюз
VLAN 95 ИБ
ISP3
Admin Internal
(аварийный доступ)
Application Firewall
Сегмент Web
(Bill Manager)
VLAN 98
Admin External
Admin Internal
Сегмент
DNS, SMTP
VLAN 99 DMZ1
ISP1
ISP1
Internet
Switch
(stack)
В бКОР
VLAN 777 Core Link
Routers
ISP2
ISP2
User
Firewall
PAM
Служебный трафик
между зонами доступности
(зависит от потребностей заказчика)
VLANs 103, 105, 102
Зона доступности N
В БКР
ЦУС

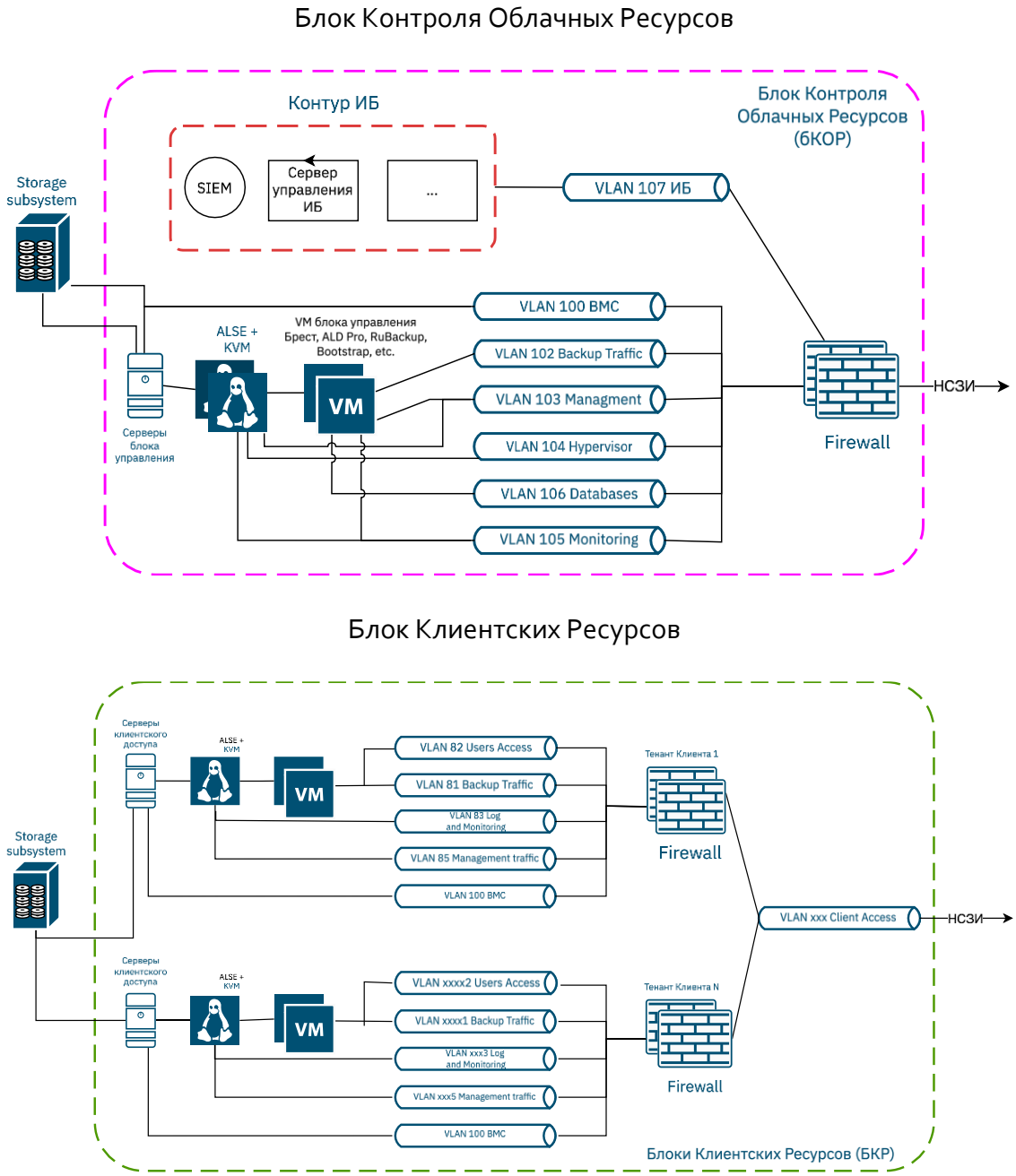


Рис.10. Комплексный пример сети

4.3 Хранение данных

ОП AIC предусматривает возможность хранения, использования и управления данными с применением различных типов систем хранения, в том числе программно-определяемых СХД (Ceph и др). Планирование подключения СХД к ОП необходимо проводить исходя из требований предъявляемых ПК СВ Брест.

Для построения облачного хранилища данных используются следующие базовые технологии хранения:

- Filesystem - файловая технология хранения;

- NFS (Network File System) - сетевая файловая система[10]
- LVM (Logical Volume Manager) - блочная технология хранения (менеджер логических томов);
- Ceph - программно-определяемое хранилище с файловым и блочным интерфейсами доступа;
- Raw Device Mapping - прямое подключение к ВМ существующих блочных устройств, используется только для организации хранилища образов;
- iSCSI-Libvirt - прямое подключение к ВМ существующих устройств iSCSI, используется только для организации хранилища образов.

Табл.8. Технологии хранения данных в ОП AIC

Технологии хранения	Методы передачи данных между хранилищем образов и системным хранилищем
Filesystem	ssh — образы копируются с помощью ssh-протокола; shared — образы экспортируются в соответствующий каталог системного хранилища на узле виртуализации; qcow2 — аналогично shared, но для образов формата qcow2. Образы создаются и передаются с помощью команды qemu-img с использованием оригинального образа в качестве опорного файла
Ceph	ceph — все образы экспортируются в Ceph-пулы; ssh — rbd-файл, ассоциируемый с образом, экспортируется в файл локальной файловой системы узла виртуализации
LVM	fs_lvm — образы хранятся как обычные файлы, при создании ВМ они выгружаются в логические тома (LV); lvm_lvm — создаются отдельные группы LVM-томов для хранилища образов и системного хранилища; lvm_thin — создаются отдельные группы LVM-томов для хранилища образов и системного хранилища, но системное хранилище организуется индивидуально для каждого узла виртуализации
Raw Devices	dev — образы представляют собой существующие блочные устройства в узлах
iSCSI libvirt	iscsi — образы представляют собой компоненты iSCSI target

Подробная информация о типах хранилищ и их настройке приведена в документации на ПК СВ «Брест».

4.3.1 Варианты использования СХД

4.3.1.1 Аппаратные СХД

При использовании аппаратных СХД, подключаемых к ОП AIC по протоколам Fibre Channel (FC) или iSCSI необходимо учитывать возможности по обеспечению надёжности и доступности, предоставляемые этими системами хранения данных.
Количество интерфейсов и контроллеров для подключения к СХД определяется архитектурой СХД. Рекомендуется использование не менее 2-х каналов (портов) для подключения к каждой системе хранения данных.

[10] Не поддерживает файловые атрибуты безопасности, использование данной ФС при построении облачного хранилища, функционирующего в мандатном контексте, недопустимо.

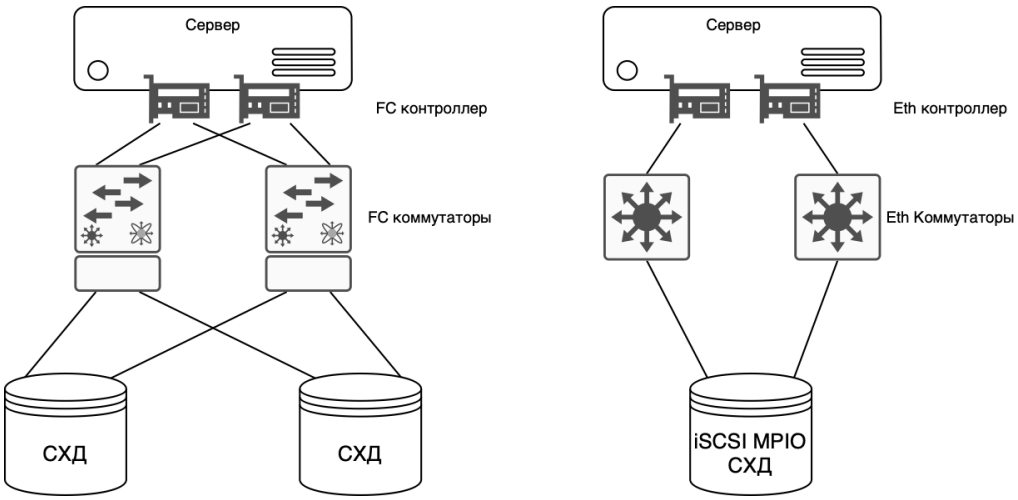


Рис.11. Пример подключения Сервера Контроля Облачных Ресурсов (СКОР) к СХД

4.3.1.2 Программно-определяемые хранилища

При необходимости использовании программно-определяемых СХД необходимо тщательное планирование ресурсов. Так же предъявляются повышенные требования к подготовке инженерного состава, обеспечивающего сопровождение системы.

Компоненты программно-определяемой СХД Ceph:

OSD (Object Storage Daemon) — это системный сервис объектного хранилища в Ceph. Предоставляет функции:

1. Хранение объектов: OSD управляет хранением объектов на локальных носителях данных (например, жёстких дисках). Обеспечивает репликацию данных для обеспечения отказоустойчивости.
2. Обеспечение доступа: OSD предоставляет доступ к объектам через сеть. Отвечает за передачу данных между клиентами и хранилищем.
3. Управление состоянием: OSD следит за состоянием данных, обнаруживает и восстанавливает повреждённые блоки. Управляет компактацией данных для оптимизации пространства.
4. Распределение данных: Ceph автоматически распределяет данные между OSD для балансировки нагрузки.

OSD — это ключевой компонент Ceph, обеспечивающий надёжное и масштабируемое хранение объектов.

MON (Monitor): MON — это системный сервис контроля в Ceph. Отвечает за следующие задачи:

1. Отслеживание состояния кластера: Мониторы следят за состоянием всех узлов в кластере, включая OSD (объектное хранилище), MDS (сервер метаданных) и другие мониторы.
2. Хранение метаданных: MON хранит информацию о состоянии кластера, конфигурации и другие метаданные.
3. Принятие решений: принимает решения о перераспределении данных, добавлении новых узлов и других аспектах управления кластером.

MDS (Metadata Server): MDS — это системный сервис сервера метаданных в Ceph. Его задача — управление метаданными файловой системы.

1. Координирование доступа к файловой системе: MDS синхронизирует доступ к общему кластеру OSD и обеспечивает целостность метаданных.
2. Управление пространством и именами файлов: Он отвечает за имена файлов, директории, разрешения и другие аспекты файловой системы.

При использовании программно-определяемой СХД (SDS) Ceph следует учитывать следующие ограничения:

В тестовой среде возможно использование серверов бКОР для запуска сервисов SDS Ceph (OSD, MON, MDS).
В продуктивных средах использование серверов бКОР для запуска сервисов SDS Ceph категорически не рекомендуется и не является поддерживаемой конфигурацией.

При установке Ceph в тестовом окружении на серверы бКОР, требуется учитывать повышенные требования к ресурсам предъявляемые этой SDS.

Использование SDS Ceph с аппаратными СХД возможно, но не может быть рекомендовано к использованию в продуктивных средах.

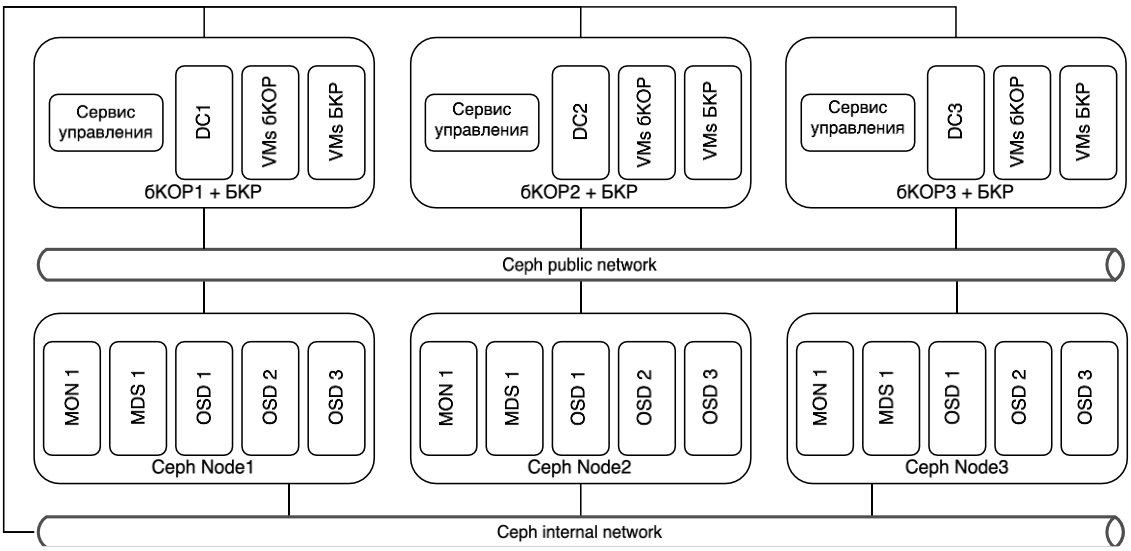


Рис.12. Пример расположения сервисов Ceph и подключения к сетям в тестовом окружении

В продуктивном окружении для установки SDS Ceph необходимо выделение отдельных физических серверов с дисками, которые будут выступать в качестве отдельного хранилища, и на которых будут запущены службы Ceph OSD. Так же требуется выделение отдельных серверов для работы служб MON и MDS.

Минимальное рекомендуемое количество серверов с MON и MDS – 3 (три) единицы.

Минимальное рекомендуемое количество серверов с OSD - 3 (три) единицы. Расчёт требований к аппаратным характеристикам каждого OSD сервера выполняется следующим образом:

- Каждый диск используемый для хранения данных — это отдельная служба OSD
- На каждый запущенный экземпляр OSD требуется минимум — 1 процессорное ядро
- На каждый 1ТБ дискового пространства на физическом диске требуется 1ГБ ОЗУ

Таким образом, в случае использования сервера с 12 дисками по 6 ТВ, для работы OSD, потребуется: минимум 12 ядер CPU и 72 ГБ RAM.

Внимание! Расчёт требуемых аппаратных ресурсов зависит от множества параметров и не может быть универсальным для всех сценариев использования Ceph. Для получения дополнительной и формации о расчёте требуемых ресурсов рекомендуется обратиться к документации Ceph.

Детальную информацию по установке и настройке SDS Ceph можно получить в справочном центре ПК СВ «Брест»

4.3.2 Резервное копирование в AIC

В качестве СРК данных для пользовательских виртуальных машин используется решение RuBackup, которое обеспечивает их хранение на стороне выделенных серверов СРК.

СРК RuBackup, обеспечивает хранение конфигурационных данных компонентов платформы и резервных копий ВМ бКОР на выделенную СХД в Блоке управления (см Рисунок N).

Архитектура СРК выполнена на основе клиент-серверной архитектуры. Минимально рекомендуемый набор компонент серверной части состоит из основного сервера, выполняющего роль управления резервным копированием и медиа сервера. Для хранения метаданных используется СУБД PostgreSQL являющаяся частью СРК.

RuBackup сервер устанавливается на выделенной виртуальной машине в Блоке Контроля Облачными Ресурсами.

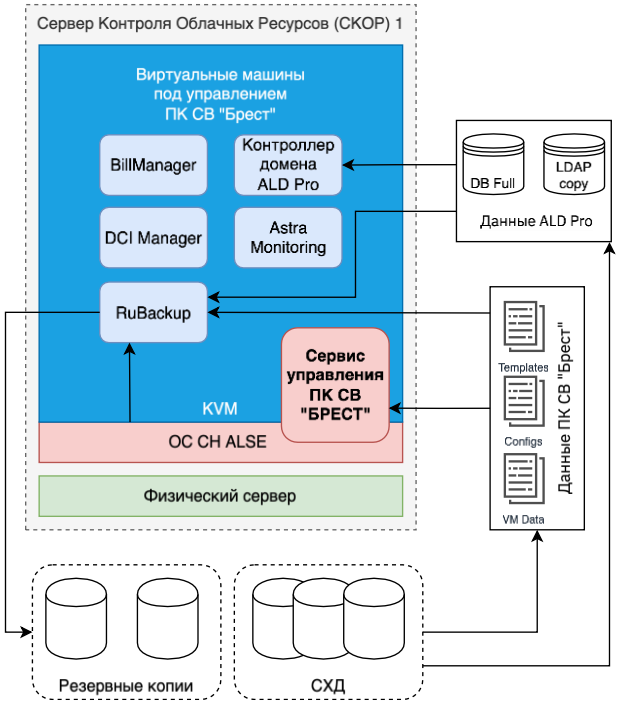


Рис.13. Схема резервного копирования платформы

В Табл.9, Табл.10, Табл.11 приведён список ресурсов, подлежащих резервному копированию.

Табл.9. Целевые объекты на уровне ОС

Ресурс	Содержимое	Источник	Расписание
/home	Содержит данные пользователей системы	Filesystem	Ежедневно, полный
/etc	Содержит конфигурационные файлы системы	Filesystem	Ежедневно, полный
/opt/rubackup/keys/	Ключи используемые для защитного преобразования резервных копий	Filesystem	Ежедневно, полный

Табл.10. Целевые объекты на уровне контроллеров домена

Ресурс	Содержимое	Источник	Расписание
База данных ALD Pro (FreeIPA) (только копия данных LDAP)	Содержит базу данных домена и его конфигурацию	ALD Pro (FreeIPA)	Ежедневно, полный
База данных ALD Pro (FreeIPA) (полная копия)	Содержит базу данных домена и его конфигурацию	ALD Pro (FreeIPA)	Еженедельно, полный

Табл.11. Таблица 8. Целевые объекты ПК СВ Брест

Ресурс	Содержимое	Источник	Расписание
Шаблоны виртуальных машин	Содержит шаблоны для создания ВМ	rubackup-brest-template	Еженедельно, полный
Виртуальные машины	Данные виртуальных машин	rubackup-brest	Еженедельно, полный
База данных PostgreSQL	Содержит конфигурацию ПК СВ Брест	rubackup-postresql	Ежедневно, полный
/var/lib/one/.one	Пароль пользователя oneadmin (необходим для восстановления БД)	Filesystem	Ежедневно, полный

4.3.2.1 Резервное копирование ВМ БКР

Базовая конфигурация RuBackup не предусматривает выполнения операций резервного копирования и восстановления виртуальных машин Блока Клиентских Ресурсов.

Для обеспечения максимального уровня отказоустойчивости и быстродействия при промышленной эксплуатации, рекомендуется использовать в качестве конфигурационной базы RuBackup СУБД PostgreSQL в отказоустойчивой конфигурации с использованием решения Patroni, развёрнутом на отдельно стоящих
машинах, построенного с использованием твердотельных накопителей, подключённых через шину PCI Express (NVMe SSD).

Для промышленных и высоконагруженных сред рекомендуется установка СРК RuBackup в многонодовой конфигурации, включающей в себя:

1. Основной сервер RuBackup
2. Резервный сервер
3. Медиа сервер(ы)

Подробная информация о рекомендуемой конфигурации компонент СРК RuBackup приведена в документации.

В случае необходимости резервное копирование образов виртуальных машин и конфигурации машин, а также параметров настройки средств виртуализации и сведений о событиях безопасности может быть реализовано с использованием встроенных средств ПК СВ «Брест», с помощью встроенных в средства виртуализации ОС СН ALSE механизмов резервного копирования (инструментов командной строки *virsh backup-begin, virsh dumpxml* и *virsh snapshot-create*), а также встроенных в ОС СН средств резервного копирования:

1) комплекс программ Bacula;
2) инструмент копирования rsync;
3) инструменты архивирования и копирования tar, cpio, gzip, cp.

4.4 Средства мониторинга

Для отслеживания работы ОП АІС используется ПО Astra Monitoring входящее в бКОР.

Astra Monitoring — это программное обеспечение, предназначенное для мониторинга продуктов Группы Астра, а также физической, виртуальной инфраструктуры, сервисов, приложений.

ПО предназначено для сбора метрик, получения и анализа файлов журналов (логов), формирования событий по предустановленным порогам, уведомления о событиях через соответствующие информационные каналы (список событий «Event List», электронная почта SMTP/POP или операционные чаты «ChatOps»).

Astra Monitoring состоит из следующих компонентов:

- клиентская часть;
- серверная часть;
- интерфейс пользователя.

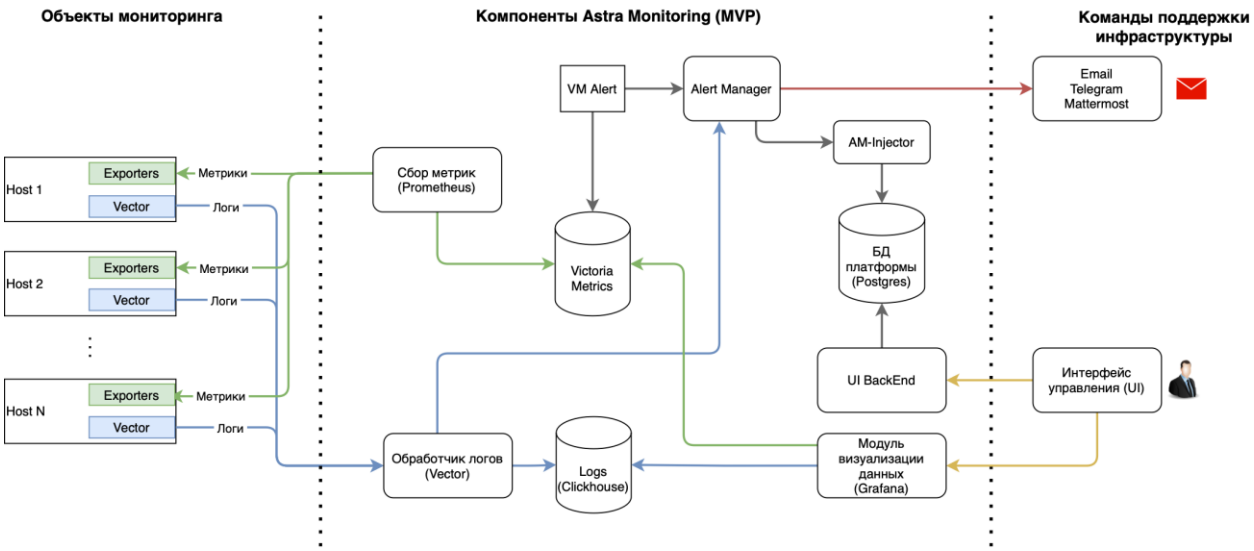


Рис.14. Компонентная схема Astra Monitoring

Интерфейс пользователя позволяет визуализировать собранные данные, отобразить метрики в виде индикаторов и графиков, предоставить информацию об обнаруженных на объектах мониторинга проблемах, добавлять объекты мониторинга в систему или удалять их и т.д.

Компоненты интерфейса:

- Модуль визуализации метрик и логов построен на базе программного продукта «Grafana», представляет из себя набор представлений данных и интерфейс анализа логов;
- Интерфейс управления - «Admin UI». Предназначен для добавления объектов мониторинга, а также для просмотра информации о событиях по объектам мониторинга.

Клиентская часть состоит из хостов - объектов мониторинга, на которые установлен набор различных экспортеров, в зависимости от роли, которую выполняют эти хосты.
Например, на сервер контроллера домена могут быть установлены «node-exporter», «systemd-exporter», «freeipa-exporter» и агент «vector» для сбора логов, а на ноду виртуализации Брест - «node-exporter», «systemd-exporter», агент «vector» и «libvirt-exporter». Установленные экспортеры собирают доступные им метрики, в зависимости от назначения экспортера, и публикуют их используя специфичный для конкретного экспортера порт, например, <host_address>:9100/metrics для «freeipa-exporter».

Компоненты клиентской части:

- Набор "Экспортеров". Обеспечивают сборку метрик и статистик наблюдаемой системы (загрузка CPU, ОЗУ, загрузку сетевых интерфейсов и т.д.).
- Программный продукт «Vector». Обеспечивает обработку и отправку логов в систему Астра Мониторинг.

Серверная часть состоит из указанных выше компонентов и предназначена для сбора, хранения и обработки данных от объектов мониторинга.
Например, компонент «Prometheus» собирает метрики путем обращения к опубликованным на объектах мониторинга экспортерам и передает их далее на хранение в базу «Victoria Metrics». Собранные в базе «Victoria Metrics» данные регулярно анализируются компонентом «vmalert» в соответствии с заданными правилами триггеров. При обнаружении соответствия

данных какому-либо правилу, «vmalert» отправляет сообщение в «alertmanager» с заданной в правиле информацией о хосте, имени правила, его кратком и полном описании, критичности и о прочих сопутствующих тегах. В «alertmanager» события группируются, обрабатываются и далее отправляются по заданным каналам оповещениями командам поддержки, а также в базу данных платформы через «am-injector» и далее в интерфейс управления.

Сбор и обработка логов производится в несколько ином порядке - установленный на объекте мониторинга агент «vector» собирает логи в соответствии с конфигурацией и отправляет их в серверную часть компонента «vector». Серверный обработчик логов «vector» производит дополнительную обработку поступающих логов, выделение и добавление ключевых полей, а также анализ поступающих данных на соответствие заданным правилам, например, ищет записи об ошибках выполнения каких-либо операций. При обнаружении подобных ошибок может быть отправлено сообщение в «alertmanager» и далее по указанной выше схеме. Собранные и обработанные логи отправляются на хранение в базу данных «Clickhouse».
Компоненты серверной части:

- Prometheus - обеспечивает сбор метрик со всех совместимых систем и сервисов.
- Vector.dev - принимает и обрабатывает лог-файлы с помощью компонентов Vector агента и сервера, который осуществляет запись полученных данных в базу данных на основе Clickhouse. Архитектура передачи данных "Vector - Vector" позволяет масштабировать систему доставки логов на сложные конфигурации дочерних подразделений.
- Victoria Metrics — обеспечивает приём метрик с объектов наблюдения, которые сохраняются в базу данных Victoria Metrics.
- Clickhouse — обеспечивает хранение данных в СУБД и за счёт сжатия они занимают меньше места, чем сырые данные. Логи категоризируются по уровню критичности события и все записи с низким уровнем критичности (info, debug, trace) помещаются в базу данных Info Logs, а записи с высоким уровнем критичности (warning, critical, error) помещаются в базу данных Critical Logs.
- PostgreSQL — система управления базой данных, которая отвечает за хранение объектов наблюдения, информации о событиях объектов мониторинга.
- AlertManager - сохраняет информацию о событиях в БД PostgreSQL через AM-Injector. Реализует отправку уведомлений о событиях в соответствующие информационные каналы (Email, Telegram, Mattermost).

Управление ПО Astra Monitoring производится из Web интерфейса, или интерфейса командной строки.

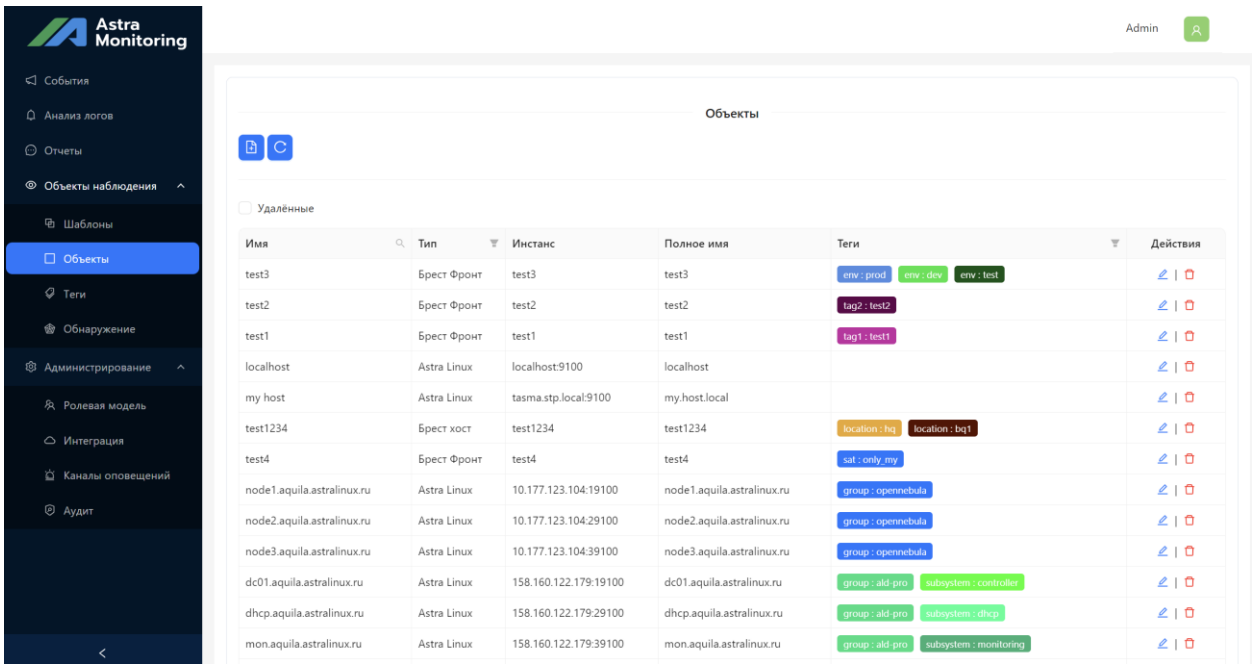


Рис.15. Web интерфейс Astra Automation

4.5 Рекомендации и варианты внедрения ОП AIC

4.5.1 Варианты установки ОП

Возможны два варианта установки ОП AIC в рамках ЦОД:

1. «Расширенный» вариант, при котором выделяется 3 (три) или более (2N+1) физических сервера Блока Контроля Облачных Ресурсов, на которых размещаются все служебные сервисы и службы ОП, и 2 (два) или более (2+N) физических сервера Блока Клиентских Ресурсов, на которых запускаются виртуальные машины пользователей ОП.
2. «Минимальный» вариант, при котором выделяется 3 (три) физических сервера Блока Контроля Облачных Ресурсов, на которых размещаются все служебные сервисы и службы ОП, и запускаются виртуальные машины пользователей ОП.

Использование варианта «Минимальный» рекомендуется для тестирования возможностей ОП, а также в том случае, если не ожидается большой нагрузки на ресурсы со стороны пользовательских виртуальных машин.

Переход от варианта «Минимальный» к варианту «Расширенный» возможен и требует выполнения следующих действий:

1. Добавление по меньшей мере 2 (двух) серверов для запуска пользовательских виртуальных машин
2. Установка ОС СН Astra Linux на новые серверы
3. Перевод новых серверов под управление ПК СВ «Брест»
4. Перенос пользовательских виртуальных машин с серверов СКОР на серверы БКР.

При выборе вариантов установки ОП AIC необходимо учитывать требования к аппаратным ресурсам, предъявляемым к различным её компонентам. Подробная информация об аппаратных требованиях указана в разделе «Требования к серверному оборудованию».

Варианты установки представлены на рис. «Расширенный» вариант установки ОП AIC и «Минимальный» вариант установки ОП AIC.

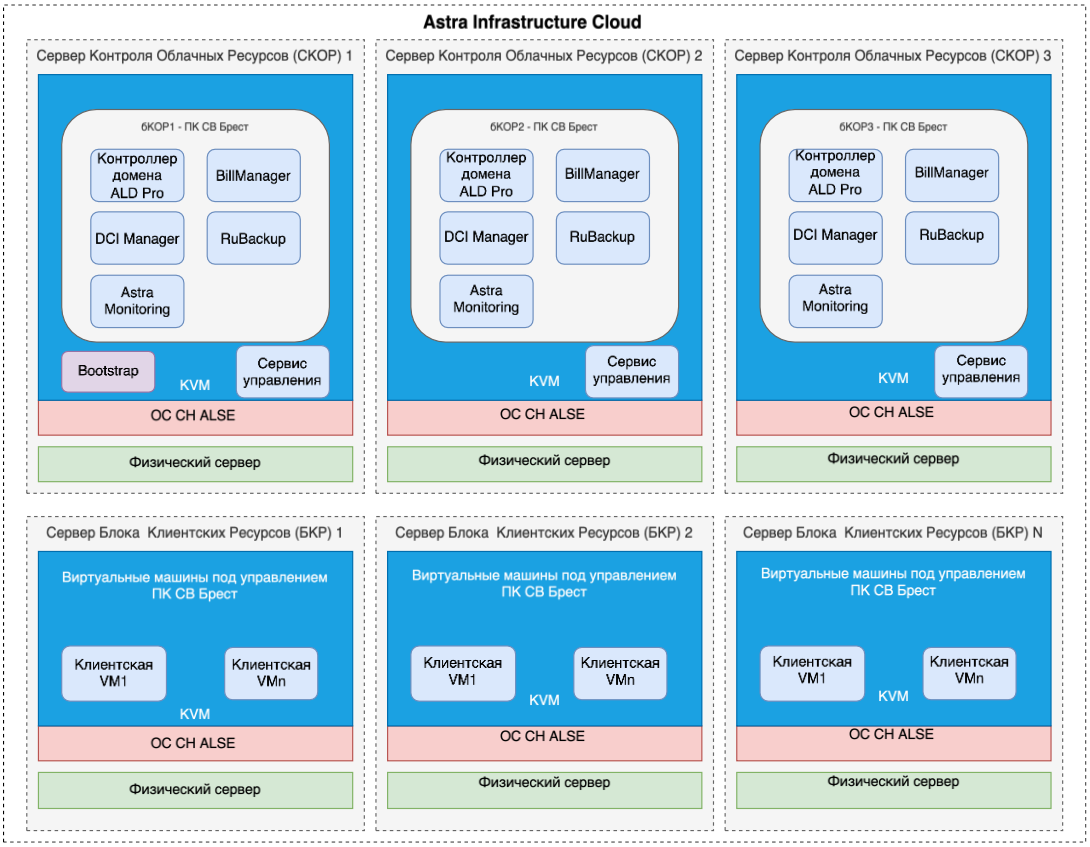


Рис.16. «Расширенный» вариант установки ОП AIC

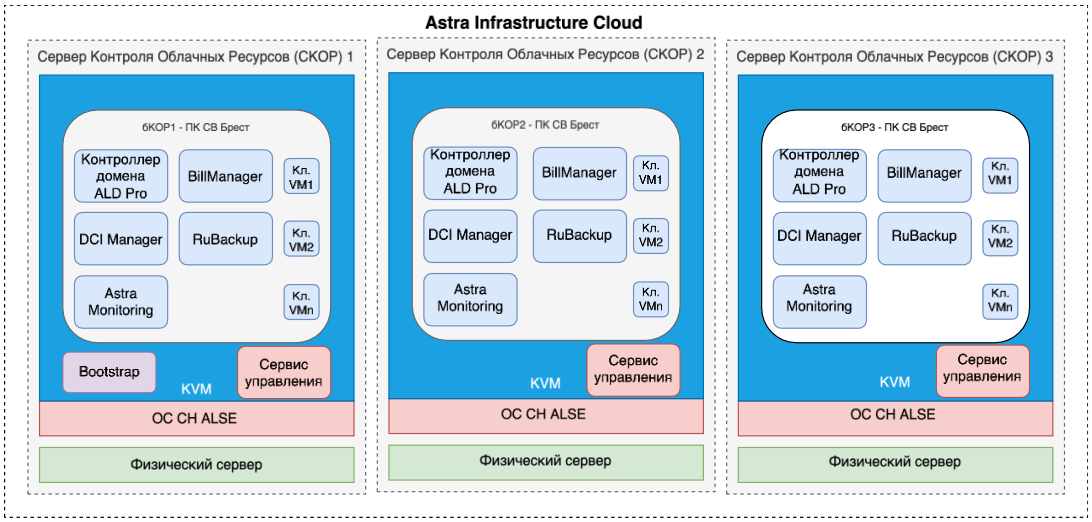


Рис.17. «Минимальный» вариант установки ОП AIC

4.5.2 Варианты установки служб ПК СВ «Брест»

Возможны два варианта установки служб ПК СВ «Брест»:

1. ПК СВ «Брест» устанавливается непосредственно поверх ОС СН Astra Linux устанавливаемой на аппаратный сервер.
2. Установка производится в виде виртуальной машины KVM

Рекомендуется использование первого варианта установки, предполагающего упрощённую конфигурацию.

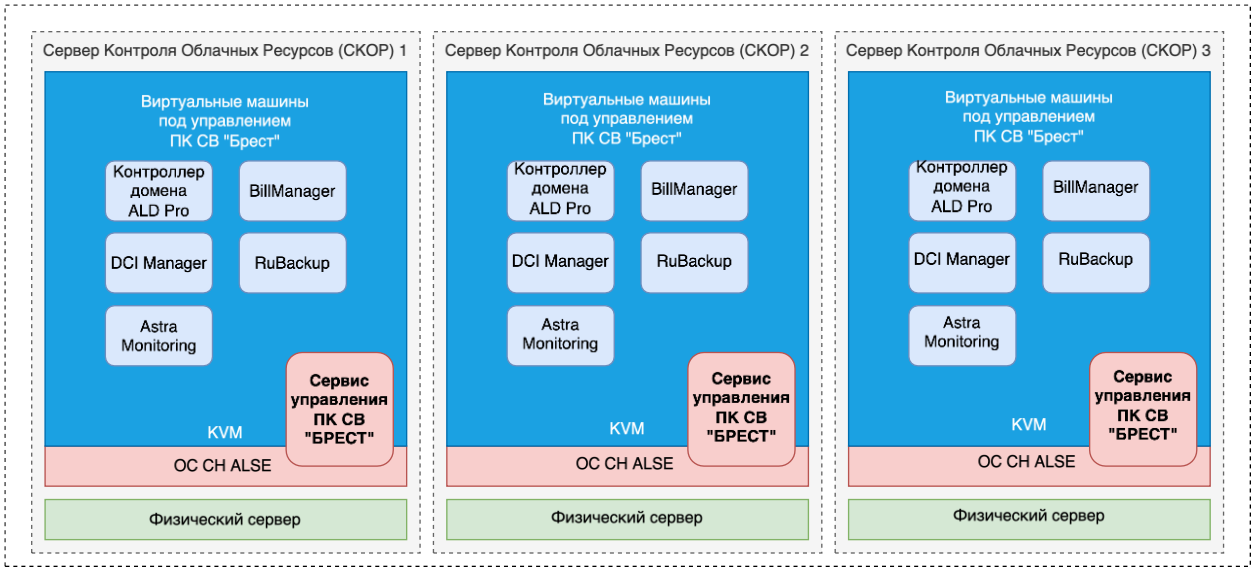


Рис.18. Вариант установки ПК СВ «Брест» в хостовую ОС

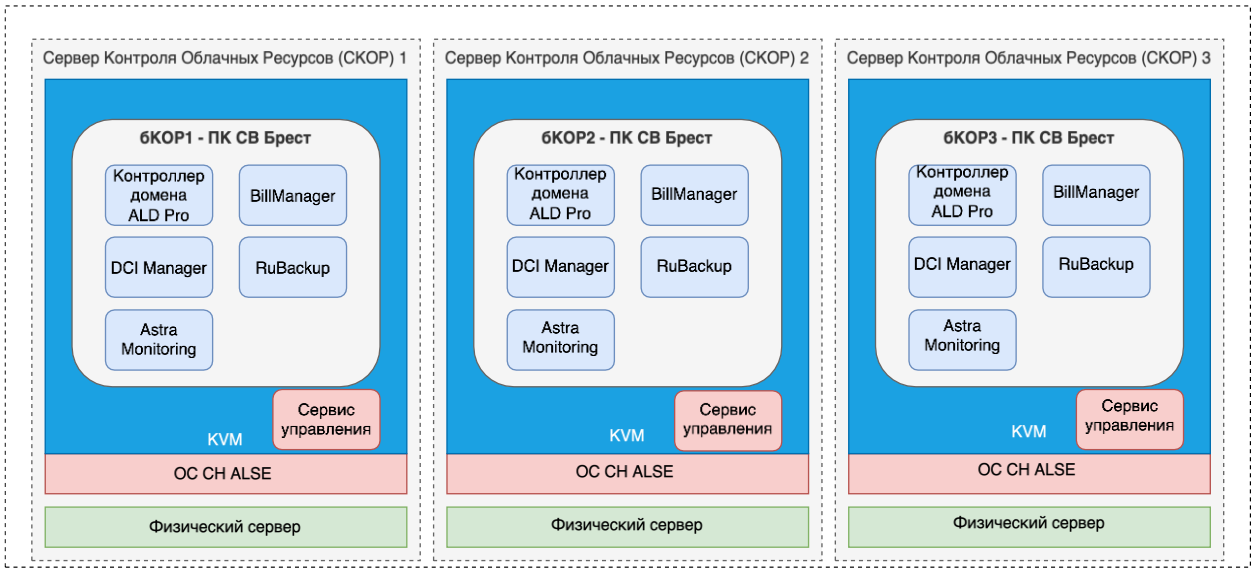


Рис.19. Вариант установки ПК СВ «Брест» в виде виртуальной машины KVM

4.5.3 Варианты размещения контроллера домена ALD Pro

При проектировании ОП AIC следует учитывать, что контроллер домена (КД) является одной из наиболее важных подсистем, на корректную работу которой завязаны все компоненты ОП.

Для обеспечения высокой доступности и отказоустойчивости службы каталогов приняты следующие решения:

- использование нескольких контроллеров домена (не менее 2-х)
- определена процедура репликации между контроллерами домена

Для обеспечения максимальной доступности служб каталога рекомендуется размещение по крайней мере одного КД за пределами ОП.

Минимально допустимое количество контроллеров домена в AIC - 3 ед.
Каждый контроллер домена должен располагаться на закреплённом за ним сервере бКОР. Перенос КД на другой сервер бКОР, на котором уже имеется работающий КД допустим в случае

выхода одного из серверов бКОР из строя, или при проведении регламентных работ по обслуживанию ОП.

В случае размещения КД ALD Pro внутри AIC рекомендуется использовать одну из предложенных ниже схем, или их вариацию.

4.5.3.1 Схема размещения №1: установка КД в независимые ВМ на KVM

Достоинства подхода:

- простота установки на уровне гипервизора KVM
- отсутствие зависимости от работоспособности ПК СВ «Брест»

Недостатки:

- Виртуальные машины КД ALD Pro, в отличии от остальных VM бКОР не находятся под управлением ОП
- Администрирование виртуальных машин выполняется средствами KVM

Порядок установки:

1. ОС СН Astra Linux
2. КД ALD Pro
3. ПК СВ Брест в дискреционном режиме

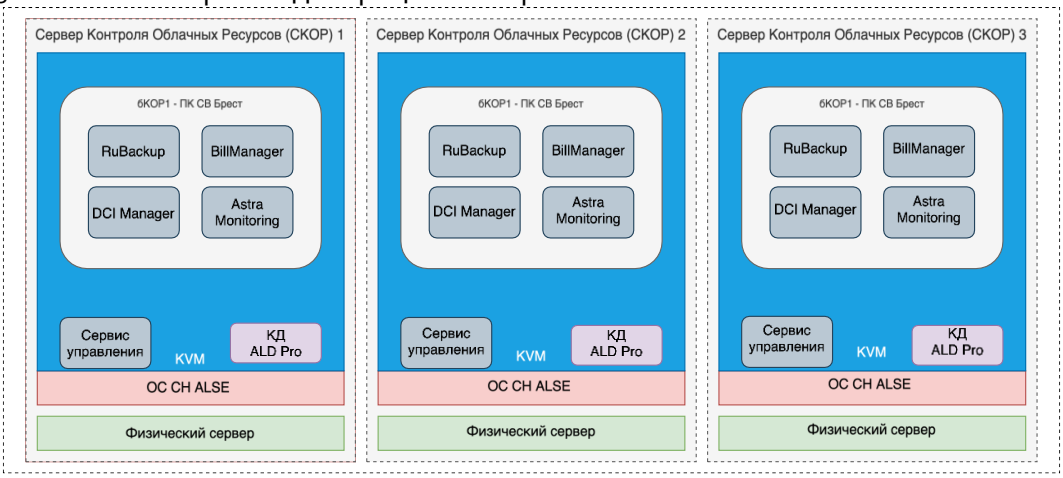


Рис.20. Установка КД в независимые ВМ на KVM

4.5.3.2 Схема размещения №2: установка КД под управлением ПК СВ «Брест»

Достоинства подхода:

- все виртуальные машины бКОР находятся под управлением ПК СВ «Брест»

Недостатки:

- относительная сложность реализации
- прямая зависимость работоспособности КД от ПК СВ «Брест»

Порядок установки:

1. ОС СН Astra Linux
2. ПК СВ Брест в сервисном режиме на 1 узел
3. КД ALD Pro в виде VM в ПК СВ «Брест» на тот же узел
4. Перенастройка ПК СВ Брест на работу с КД (перевод в дискреционный режим)
5. Добавление 2-х узлов ПК СВ Брест

6. Установка 2-х КД ALD Pro в виде VM в ПК СВ Брест

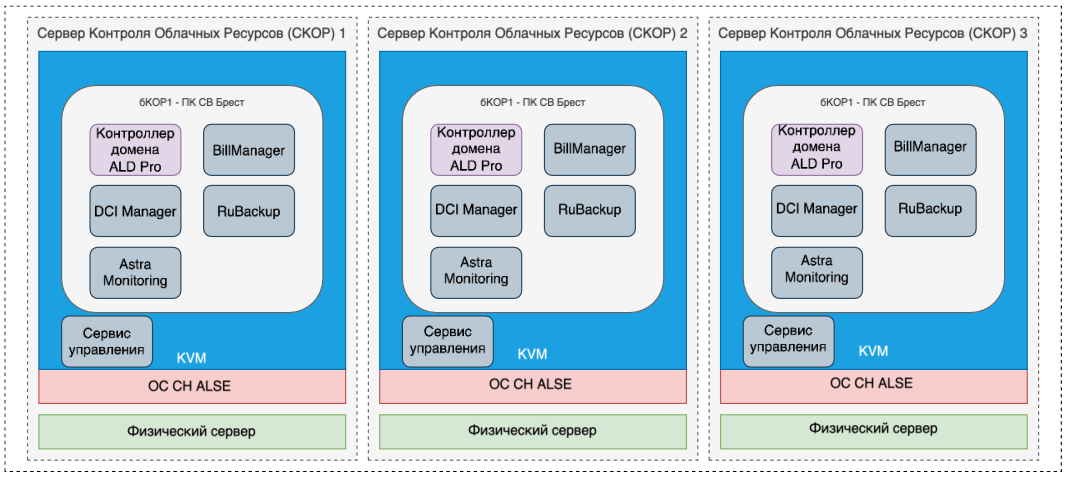


Рис.21. Установка КД под управлением ПК СВ «Брест»

4.5.3.3 Схема размещения №3: установка КД в гибридном режиме

Достоинства подхода:

- простота реализации

Недостатки:

- относительная сложность администрирования
- экземпляры VM КД находятся в разных доменах управления

Порядок установки:

1. ОС СН Astra Linux
2. КД ALD Pro
3. ПК СВ «Брест» в дискреционном режиме
4. Установка 2-х КД ALD Pro в виде VM в ПК СВ «Брест»

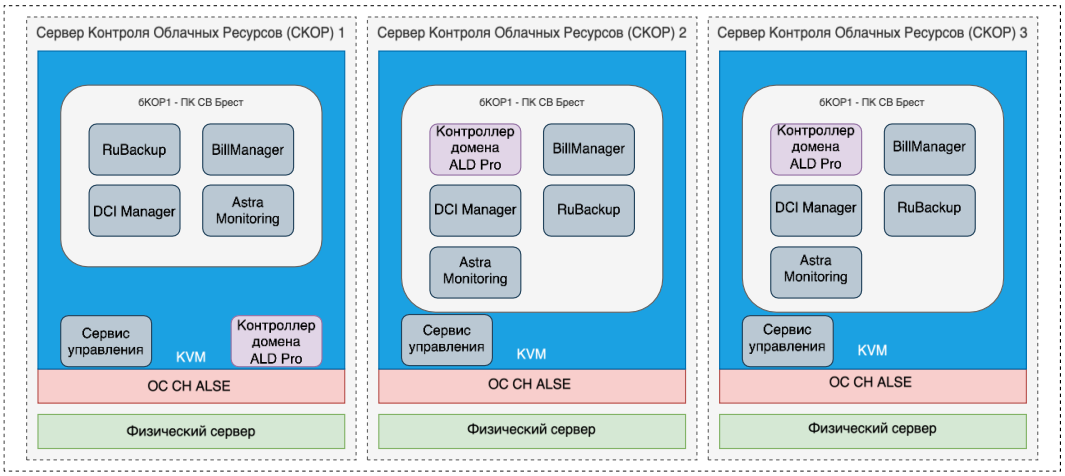


Рис.22. Установка КД в гибридном режиме

4.5.4 Варианты подключения СХД к AIC

В продуктивных средах, при необходимости использования программно-определяемых СХД, таких как Ceph, необходимо использовать конвергентный подход, при котором предполагается разделение вычислительных ресурсов и систем хранения данных на отдельные, доступ-

ные по требованию пулы. Использование такого подхода позволит выстроить гибкую и управляемую инфраструктуру одновременно повысив доступность всей системы в целом, снизив возможные взаимные негативные влияния компонент.

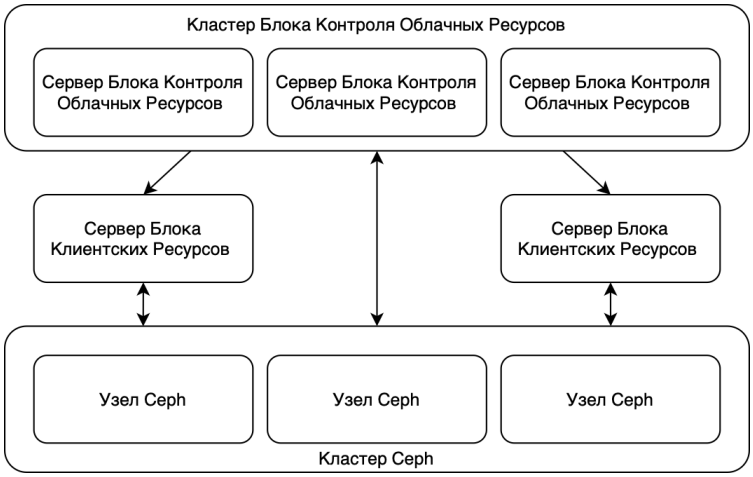


Рис.23. Вариант конвергентной конфигурации с использованием Ceph.

4.6 Архитектурные требования и ограничения

4.6.1 Гиперконвергентные системы

К гипервонвергентным системам в ОП AIC относятся конфигурации, в которых используется программно-определяемая система хранения данных (SDS), а компоненты SDS используют те же вычислительные ресурсы (серверы), что и Блок Контроля Облачных Ресурсов (бКОР) и (или) Блока Клиентских Ресурсов (БКР).

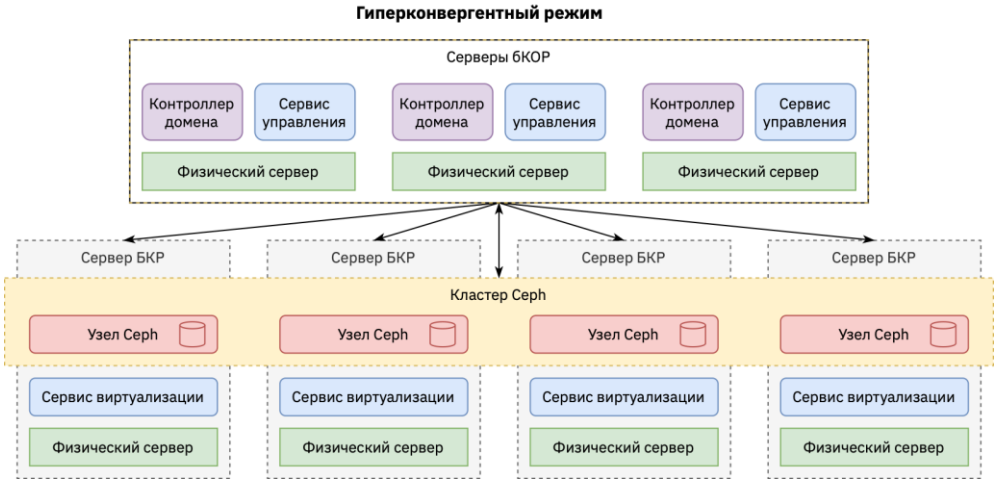


Рис.24. Пример гиперконвергентной конфигурации

При использовании программно-определяемой СХД Ceph необходимо учитывать требования к ресурсам предъявляемым этой SDS.

В тестовой среде возможно использование серверов бКОР для запуска сервисов SDS Ceph (OSD, MON, MDS).

Внимание! В продуктивных средах использование серверов бКОР и(или) БКР для запуска сервисов SDS Ceph категорически не рекомендуется и не является поддерживаемой конфигурацией.

4.6.2 СРК RuBackup

На момент написания этого документа RuBackup не поддерживает доменную аутентификацию пользователей в КД ALDPro.

5 Масштабирование

Выбор ресурсов для масштабирования определяется потребностями в том или ином типе ресурсов и текущей загрузки серверов ОП AIC. В общем случае, сигналом о необходимости масштабирования служит загрузка ресурсов на 75-80 и более процентов (требуется настройка соответствующих триггеров в Astra Monitoring). Так же необходимо учитывать расчётный всплеск нагрузки на облачные ресурсы, определяемый сезонностью и другими факторами.

Внимание! Добавление новых серверов и новых экземпляров ПО может потребовать приобретения дополнительных лицензий.

5.1 Масштабирование Блока Контроля Облачных Ресурсов

Увеличение количества серверов БКОР производится исходя из формулы:

- общее количество серверов = 2N+1.

Добавление новых серверов в бКОР может быть обусловлено следующими факторами:

- увеличение нагрузки на серверы за счёт увеличения количества служебных сервисов;
- повышение доступности бКОР за счёт увеличения количества узлов входящих в RAFT кластер.

После добавления новых серверов в бКОР необходимо произвести добавление инстансов служб ОП, требующих масштабирования. К таковым могут относиться: сервис управления ПК СВ «Брест», КД ALDPro, RuBackup, DCImanager и пр. Масштабирование должно производиться исходя из требований программных продуктов входящих в ОП. Подробная информация доступна в документации к программным продуктам составляющим ОП AIC.

5.2 Масштабирование Блока Клиентских Ресурсов

В общем случае, увеличение ёмкости БКР может быть произведено путём вертикального, либо горизонтального масштабирования.

При вертикальном масштабировании, в уже имеющиеся серверы БКР производится установка дополнительных модулей оперативной памяти, процессоров, дисков или сетевых контроллеров.

При горизонтальном масштабировании увеличение количества доступных ОП ресурсов производится путём добавления новых серверов. В случае добавления вычислительных мощностей в существующий VDC, минимальное количество новых серверов составляет 1 ед. При необходимости создания нового тенанта, минимальное количество добавляемых серверов - 2 ед.

При добавлении новых серверов необходимо учитывать архитектурные особенности реализации ОП, такие как минимальное количество контроллеров, дисков, RAM и пр.

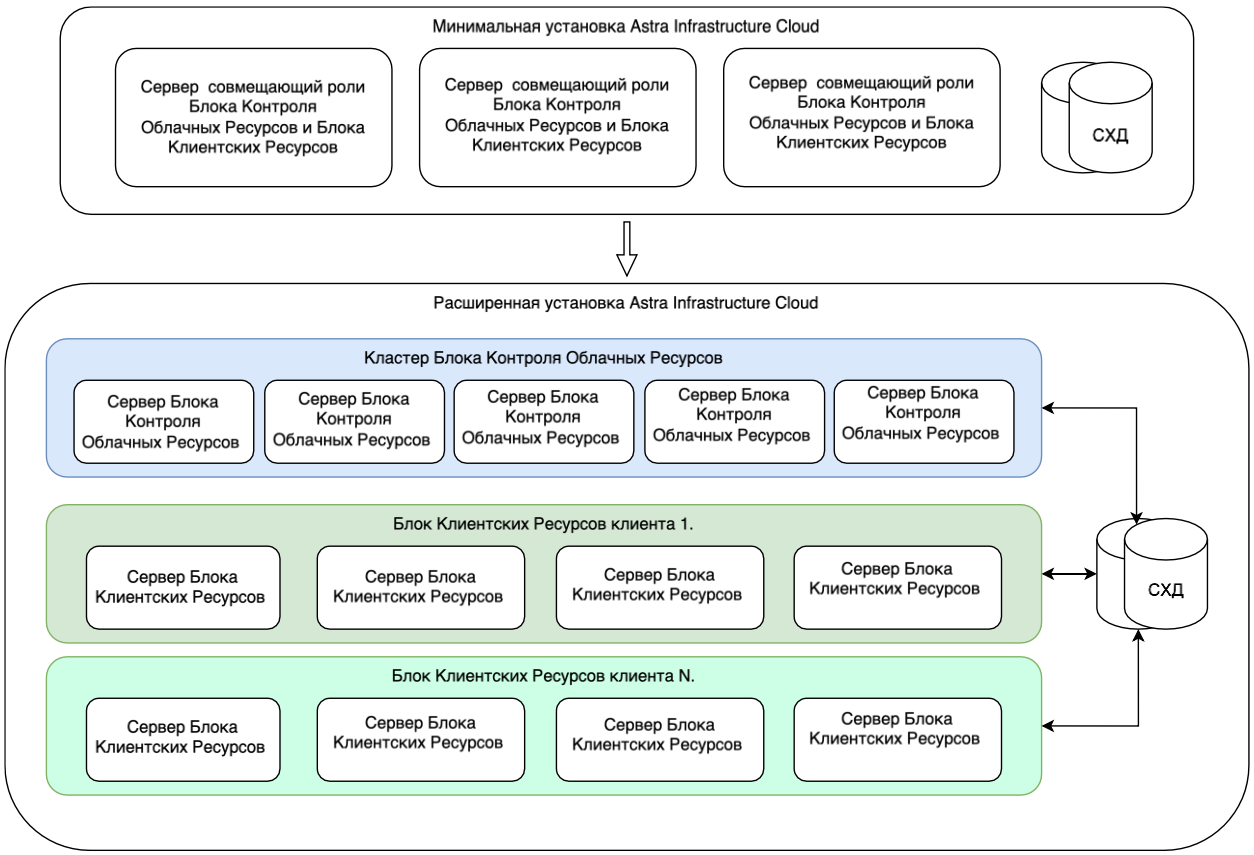


Рис.25. Вариант масштабирования ОП AIC

6 Интеграция с внешними системами

6.1 Интеграция со службами Active Directory

При установке ОП AIC обязательным требованием является использование службы каталогов, построенной на базе ALD Pro или Freeipa. При этом в организации уже может использоваться сервис доменов на основе Microsoft Active Directory (MS AD).
В домене MS AD могут находится компьютеры с операционной системой Windows. Для корректной работы пользователей, зарегистрированных в домене MS AD с AIC необходима возможность гибридной работы пользователей сразу в двух доменах с помощью механизма доверительных отношений.
В ALD Pro реализована возможность использования двусторонних доверительных отношений за счёт использования механизма глобального каталога.
Подробная информация по настройке доверительных отношений доступна в документации ALD Pro

7 Приложения

7.1 Приложение 1. Список сетевых портов, используемых компонентами AIC

7.1.1 Приложение 1.1 Сетевые порты используемые ПК СВ Брест

Табл.12. Сетевые порты используемые ПК СВ Брест

Порт	Протокол	Прикладной Протокол	Комментарий
22, 2633	TCP/UDP	SSH, API XML-RPC	Между хостами ПК СВ «Брест», двусторонние связи
80, 443, 2616	TCP	HTTP/HTTPS	Между хостами ПК СВ «Брест» и всеми ВМ для установки утилиты управления.
29876, 5900-7000	TCP	Служба протокола SPICE для виртуальных машин	Между хостами ПК СВ Брест и всеми ВМ, доступ к ВМ из интерфейса ПК СВ «Брест»
5900, 80, 443	TCP	HTTP/HTTPS SPICE	Между хостами ПК СВ «Брест» и всеми ВМ
53	UDP	При условии использования AD существующей инфраструктуры	Между хостами ПК СВ «Брест» и всеми ВМ
2474, 5030	TCP/UDP	Взаимодействие между ВМ и ПК СВ «Брест»	Между хостами ПК СВ «Брест» и всеми ВМ для обмена технической информацией.
21	TCP	FTP	Между хостами ПК СВ «Брест», двусторонние связи и Сервисными ВМ
623	UDP	IPMI	Между хостами ПК СВ «Брест», двусторонние связи, для функционирования технологии горячего резервирования.
443, 80	TCP		
123	UDP	NTP	Между хостами ПК СВ «Брест» и всеми ВМ для синхронизации времени.
4124	TCP/UDP	Мониторинг хостов	Между хостами ПК СВ «Брест»
443, 80, 22	TCP	HTTP/HTTPS, SSH	Доступ с компьютера администратор/инженера для установки и настройки ПК СВ «Брест»

7.1.2 Приложение 1.2 Сетевые порты используемые ALD Pro

Табл.13. Сетевые порты используемые ALD Pro

Порт	Протокол	Прикладной протокол	Комментарий

80 (443)	TCP	HTTP(S)	Портал управления, REST API
389 (636)	TCP	LDAP(S)	Репликация между контроллерами, запросы со стороны SSSD на клиентских ПК, обращения от пользовательских приложений.
88	TCP/UDP	Kerberos	Аутентификация в домене
464	TCP/UDP		Смена пароля
53	TCP/UDP	DNS	Разрешение имен, запросы от SSSD на динамическое обновление записей
135, 139	TCP	NetBIOS	NetBIOS нужен для работы доверительных отношений с MS AD
137 и 138	UDP		
445	TCP	SMB2	SMB выступает транспортом для RPC вызовов, которые используются, например, для удаленного обращения к LDAP каталогу при разрешении идентификаторов, или во время создания доверительных отношений.
123	UDP	NTP (Chrony)	Синхронизация времени на хостах в домене. На контроллере служба chrony открывает также порт 323/TCP, но он нужен только для управления сервисом через утилиту chronyc
4505 и 4506	TCP	SaltStack	Подключение к шине ZeroMQ для получения заданий автоматизации и групповых политик.

7.1.3 Приложение 1.3 Сетевые порты используемые RuBackup

Табл.14. Сетевые порты используемые RuBackup

Компонент		Целевой сервис	Протокол	Порт	Описание
От	До				
Основной сервер	Медиасервер	rubackup-cmd	TCP	9991	Управление операциями на медиасервере
		rubackup-media	TCP	9993	Управление операциями с данными
Основной сервер	База данных RuBackup на отдельностоящей машине	postgresql	TCP	5432	Сохранение конфигурационной и оперативной информации

Резервный сервер	Основной сервер	rubackup-cmd	TCP	9991	Обеспечение отказоустойчивости
		rubackup-media	TCP	9993	Передача данных между медиасеурверами в составе основного и резервного серверов
Резервный сервер	База данных RuBackup на отдельностоящей машине	postgresql	TCP	5432	Сохранение конфигурационной и оперативной информации
Медиасервер	Медиасервер	rubackup-media	TCP	9993	Передача данных между медиасерверами
Медиасервер	Резервный сервер	rubackup-cmd	TCP	9991	Управление операциями на медиасервере
		rubackup-media	TCP	9993	Управление операциями с данными
Медиасервер	База данных RuBackup на отдельностоящей машине	postgresql	TCP	5432	Сохранение конфигурационной и оперативной информации
Клиент резервного копирования	Основной сервер	rubackup-cmd	TCP	9991	Управление операциями на клиенте резервного копирования
Клиент резервного копирования	Медиасервер	rubackup-media	TCP	9993	Передача данных между медиасервером и клиентом
Клиент резервного копирования	Резервный сервер	rubackup-cmd	TCP	9991	Управление операциями на клиенте резервного копирования
		rubackup-media	TCP	9993	Передача данных между медиасервером и клиентом
RuBackup REST API	Основной сервер	rubackup-rbm	TCP	9995	Отправка запросов на сервер и получение информации

RuBackup REST API	База данных RuBackup на отдельностоящей машине	postgresql	TCP	5432	Получение информации из базы данных
RuBackup REST API	Резервный сервер	rubackup-rbm	TCP	9995	Отправка запросов на сервер и получение информации
Менеджер RuBackup (RBM) на отдельно стоящей машине	База данных RuBackup на отдельностоящей машине	postgresql	TCP	5432	Сохранение конфигурационной и оперативной информации
Менеджер RuBackup (RBM) на отдельно стоящей машине	Основной сервер	rubackup-rbm	TCP	9995	Управление операциями RuBackup
Менеджер RuBackup (RBM) на отдельно стоящей машине	Резервный сервер	rubackup-rbm	TCP	9995	Управление операциями RuBackup
Клиент, посылающий запрос через Rubackup REST API	Основной сервер	rubackup-api	HTTPS	443	Управление операциями RuBackup через REST API
Клиент, посылающий запрос через Rubackup REST API	Резервный сервер	rubackup-api	HTTPS	443	Управление операциями RuBackup через REST API

7.2 Приложение 1.4 Сетевые технологии и топология

7.2.1 Сетевая архитектура и технологии

Архитектура физической сети ОП AIC строится на двухуровневой топологии Spine and Leaf с резервированием и с максимальной реализацией принципа отсутствия единой точки отказа.

Данная архитектура обеспечивает возможность передавать большое количество трафика восток-запад внутри ЦОД на максимальной скорости, которую предоставляют линии связи, с одинаковой минимальной прогнозируемой задержкой. Это обеспечивается тем, что от источника до цели трафик всегда проходит одинаковое количество промежуточных сетевых устройств.

Уровень Leaf состоит из коммутаторов уровня доступа, которые обеспечивают подключение клиентских устройств без обработки трафика на третьем уровне. В каждой серверной стойке предполагается установка двух Leaf коммутаторов, которые объединяются в MLAG (Multi-Chassis Link Aggregation) пару для отказоустойчивости, клиентские устройства подключаются с помощью протокола агрегации каналов в оба коммутатора двумя и более линиями связи параллельно.
Коммутаторы уровня Spine объединяют все коммутаторы уровня доступа в full-mesh топологию и производят обработку трафика на третьем уровне.

Логически сеть облака разделяется на два уровня:

Underlay (базовая) сеть - физическая высокоскоростная отказоустойчивая сеть, построенная по топологии Spine and Leaf, основной задачей которой является передача трафика между клиентскими устройствами, быть легко масштабируемой с минимумом изменений в конфигурационных файлах сетевых устройств. Протокол динамической маршрутизации BGP используется для передачи маршрутной информации между сетевыми устройствами.

Overlay (виртуальная) сеть - логическая сеть, которая строится поверх физической сети. Оверлейные сети создаются путем инкапсулирования трафика и его туннелирования в физической сети. Протокол туннелирования VXLAN инкапсулирует Ethernet-кадры уровня 2, поступающие от клиентских устройств, в UDP-пакеты уровня 3, активируя виртуальные сети уровня 2. Инкапсуляция и декапсуляция VXLAN производится конечными устройствами туннеля VXLAN (VTEP - Vitual Tunnel End Point). EVPN (Ethernet VPN) — это расширение протокола BGP, которое позволяет сети передавать информацию о доступности конечного устройства, такую как MAC-адреса уровня 2 и IP-адреса уровня 3. Эта технология плоскости управления использует MP-BGP (Multiprotocol BGP) для распределения MAC-адресов и IP-адресов конечных устройств, где MAC-адреса рассматриваются как маршруты. EVPN позволяет VTEP устройствам обмениваться между собой информацией о доступности конечных устройств.

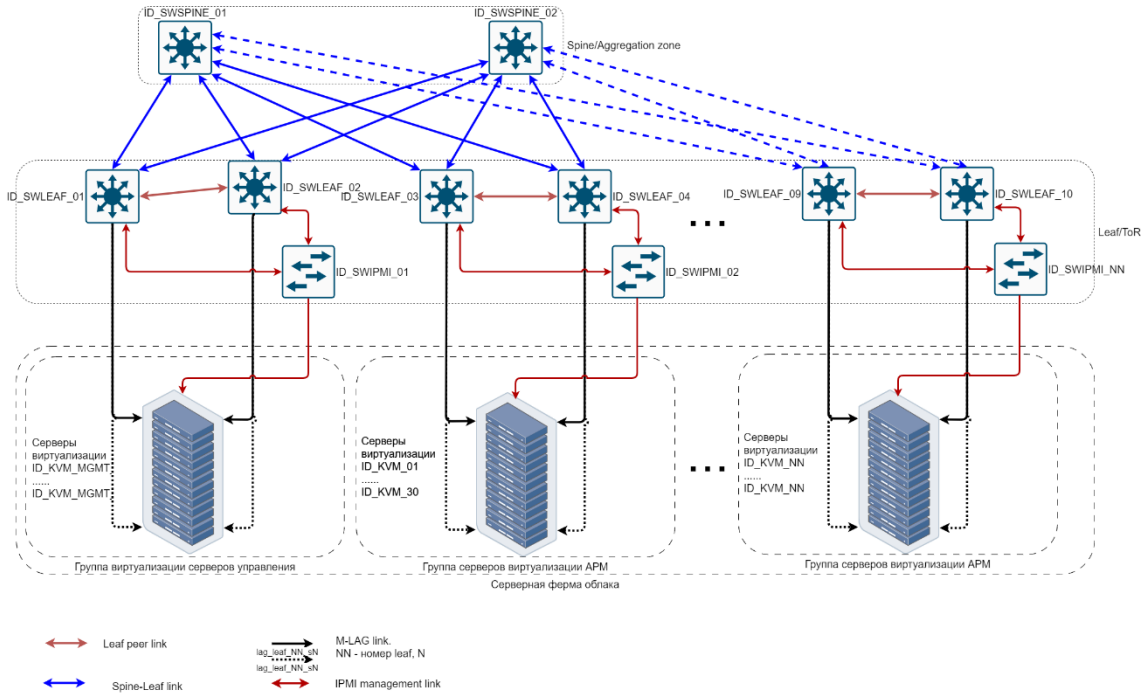


Рис.26. Структурная схема сети

На Рис.26 отображается сопряжения ключевых физических элементов, обеспечивающих функционирование облачной инфраструктуры.
На последующих схемах будут отображаться 2 (два) коммутатора уровня Spine и 4 (четыре) коммутатора уровня Leaf. Предполагается, что дальнейшее горизонтальное масштабирование инфраструктуры выполняется аналогичным образом с соответствующими изменениями в планах адресации и коммутации.

Табл.15. Пример распределения VLAN

Номер VLAN	Наименование VLAN	Описание
10	FW-Inside	Сегмент сети межсетевого экрана в сторону облака
11	FW-Outside	Сегмент сети межсетевого экрана во внешнюю сеть
101	MGMT	Сеть управления
102	KVM	Сеть гипервизоров
103	IPMI	Сеть IPMI
104	CEPH	Сеть CEPH (в случае использования)
105	VM	Сеть трафика виртуальных машин
200	RUBACKUP	Сеть RuBackup

7.2.2 Топология второго уровня

На схеме отображается формирования каналов связи между элементами облачной инфраструктуры.

На Рис.27 отображены 2 (два) коммутатора уровня Spine и 4 (четыре) коммутатора уровня Leaf. Предполагается, что дальнейшее горизонтальное масштабирование инфраструктуры выполняется аналогичным образом с соответствующими изменениями в планах адресации и коммутации.

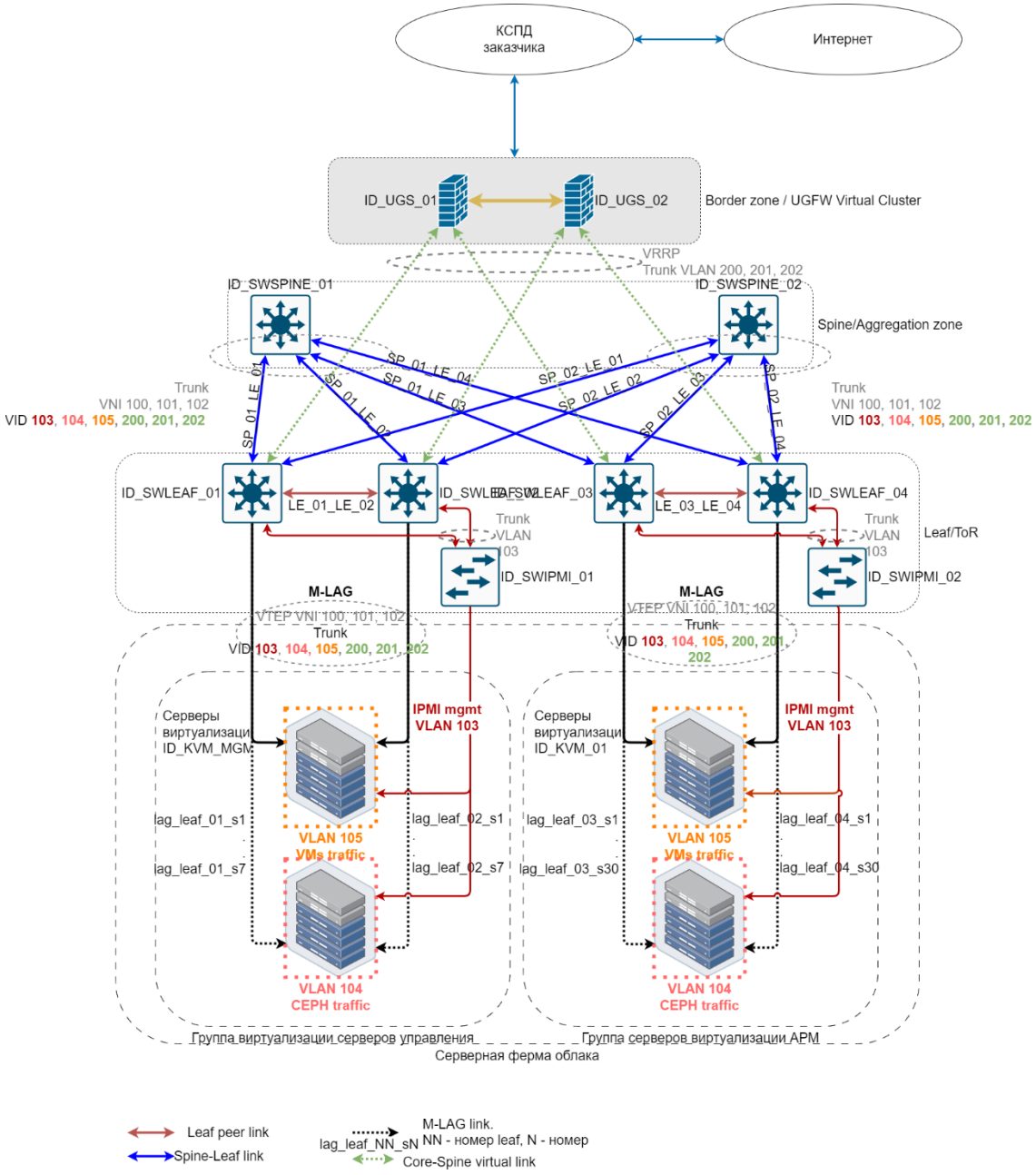


Рис.27. Схема уровня сетевых каналов (L2)

7.2.3 Топология третьего уровня

Разрабатываемая инфраструктура частного облака предполагает кооперативное использование имеющихся вычислительных ресурсов всеми пользователями и информационными системами. Для повышения управляемости и безопасности систем в инфраструктуре реализуется функционал тенантов - логических сущностей, позволяющих разделить ресурсы и предоставляемые сервисы. В частности, одним из таких сервисов является обеспечение сетевой связности с внешними сетями Корпоративной сети передачи данных (КСПД) и интернет. Согласно

техническому заданию, связность информационных систем, расположенных в разрабатываемой облачной инфраструктуре, с внешними сетями должна обеспечиваться с использованием кластера виртуальных межсетевых экранов (МЭ).
Рис.28 отображает схему сетевого уровня (L3), где отображается формирования каналов связи между элементами облачной инфраструктуры.
На схеме отображены два коммутатора уровня Spine и 4 (четыре) коммутатора уровня Leaf.
Предполагается, что дальнейшее горизонтальное масштабирование инфраструктуры выполняется аналогичным образом с соответствующими изменениями в планах адресации и коммутации.
Для выполнения требований в рамках проектирования необходимо реализовать следующие технические решения:
Технологический тенант виртуального Межсетевого Экрана (МЭ):
Кластер виртуальных МЭ разворачивается в выделенном тенанте в инфраструктуре разрабатываемого частного облака.
Внешний виртуальный интерфейс кластера необходимо коммутировать с использованием возможностей средств виртуализации и физической сетевой инфраструктуры (VLAN/VXLAN) облака таком образом, чтобы обеспечить доставку трафика до точки физического сопряжения сетевой инфраструктуры облака с КСПД. IP-адрес внешнего виртуального интерфейса кластера должен принадлежать адресному пространству КСПД.
Внутренний интерфейс кластера виртуальных МЭ необходимо сконфигурировать таким образом, чтобы с использованием возможностей средств виртуализации и физической сетевой инфраструктуры (VLAN/VXLAN) до него осуществлялась доставка маркированного трафика. Маркировка осуществляется с использованием VID тегов (VLAN ID) в соответствии с адресным планом.
Для обеспечения функций маршрутизации и фильтрации трафика для каждого уникального VID на внутреннем интерфейсе виртуального МЭ должен быть сформирован дочерний (sub) интерфейс и назначен IP-адрес из технологического диапазона, выделенного исключительно для целей подключения тенантов информационных систем.
При формировании инфраструктуры тенанта информационной системы необходимо создать виртуальный пограничный маршрутизатор для обеспечения связности сети тенанта и внутреннего интерфейса виртуального МЭ. Созданный пограничный маршрутизатор тенанта должен быть настроен для обеспечения маршрутизации трафика с сетью тенанта. Внешний интерфейс пограничного виртуального маршрутизатора тенанта необходимо коммутировать с использованием возможностей средств виртуализации и физической сетевой инфраструктуры (VLAN/VXLAN) облака таком образом, чтобы обеспечить доставку трафика до внутреннего дочернего (sub) интерфейса кластера виртуальных МЭ в соответствии с назначенным VID.

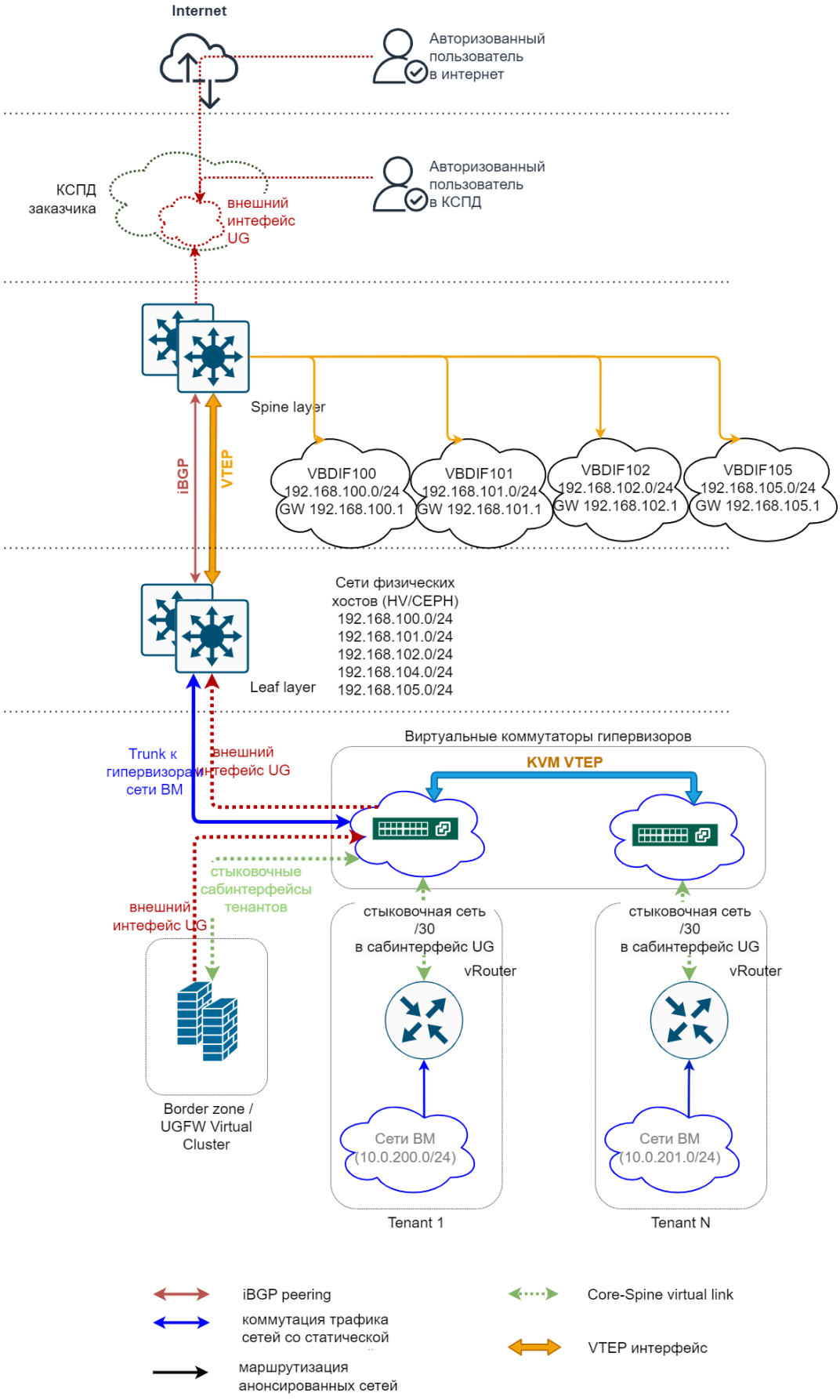


Рис.28. Схема сетевого уровня L3

7.3 Приложение 2. Лицензирование[11]

Табл.16. Список необходимых лицензий для ОП AIC вариант «Базовый»

Компонент	Описание	Кол-во	Производитель
ПК СВ «Брест»	Лицензия на Программный комплекс «Средства виртуализации «Брест», РДЦП.10001-02, для Linux и Windows (Брест Корпоратив), способ передачи электронный, до 2 сокетов с неограниченным количеством ВМ и операционную систему специального назначения «Astra Linux Special Edition» для 64-х разрядной платформы на базе процессорной архитектуры x86-64,(очередное обновление 1.7) уровень защищенности «Максимальный» («Смоленск»), РУСБ.10015-01 (ФСТЭК), способ передачи электронный, серверная до 2 сокетов, на срок действия исключительного права, с включенными обновлениями Тип 2 на 36 мес.	3	ООО "РусБИТех-Астра"
	Сертификат технической поддержки на Программный комплекс «Средства виртуализации «Брест» для Linux и Windows (Брест Корпоратив), для 1 сервера до 2 сокетов, тип «Привилегированная», на 24 мес.	3	ООО "РусБИТех-Астра"
ALD Pro	Лицензия на Программный комплекс "ALD Pro" РДЦП.10101-01 на 1 устройстве и операционную систему специального назначения «Astra Linux Special Edition» для 64-х разрядной платформы на базе процессорной архитектуры x86-64 РУСБ.10015-01 (ФСТЭК) на 8 устройствах, способ передачи электронный, для сервера, на срок действия исключительного права, с включенными обновлениями Тип 2 на 36 мес.	2	ООО "РусБИТех-Астра"
	Лицензия клиентская, на подключение 1 устройства к Программному комплексу "ALD Pro" РДЦП.10101-01, способ передачи электронный, на срок действия исключительного права, с включенными обновлениями Тип 2 на 36 мес.	50	ООО "РусБИТех-Астра"
	Сертификат технической поддержки тип «Привилегированная» на Программный комплекс "ALD Pro" для 1 сервера, на 24 мес.	2	ООО "РусБИТех-Астра"
		50	ООО "РусБИТех-Астра"
RuBackup	Лицензия на систему резервного копирования "RuBackup", способ передачи электронный, включает 1ТБ полных уникальных резервных копий, front-end, от 1 до 100 ТБ, на срок действия исключительного права, с включенными обновлениями Тип 2 на 36 мес.	2	ООО «РУБЭКАП»
	Сертификат технической поддержки на 1ТБ системы резервного копирования "RuBackup", способ передачи электронный, для полных уникальных резервных копий, front-end, от 1 до 100 ТБ, тип "Привилегированная", на 24 мес	2	ООО «РУБЭКАП»
	Для бесплатного использования системы резервного копирования RuBackup доступна лицензия, позволяющая выполнять резервное копирование и восстановление суммарным объемом резервных копий не более 1Тб. Эта лицензия включена в серверный пакет RuBackup.	2	ООО «РУБЭКАП»

[11] Требуется перепроверка и согласование количества лицензий для каждой поставки ОП AIC.

DCImanager	Лицензия на программное обеспечение DCImanager 6 редакции Infrastructure на 1 master-сервер, способ передачи электронный	1	АО "ЭКЗОСОФТ"
	Расширение лицензии на программное обеспечение DCImanager 6 редакции Infrastructure на 1 единицу оборудования, способ передачи электронный, на срок действия исключительного права, с включенными обновлениями Тип 2 на 36 мес.	10	АО "ЭКЗОСОФТ"
	Лицензия на модуль "Учет оборудования" на 5000 единиц оборудования для программного обеспечения DCImanager 6 редакции Infrastructure, способ передачи электронный, на срок действия исключительного права, с включенными обновлениями Тип 2 на 36 мес.	1	АО "ЭКЗОСОФТ"
	Сертификат технической поддержки и обновления на программное обеспечение DCImanager 6 редакции SE на 1 единицу оборудования, тип "Привилегированная", на 24 мес	10	АО "ЭКЗОСОФТ"
	Сертификат технической поддержки и обновления на модуль "Учет оборудования" на 5000 единиц оборудования для программного обеспечения DCImanager 6 редакции Infrastructure, тип "Привилегированная", на 24 мес	1	АО "ЭКЗОСОФТ"

Табл.17. Список необходимых лицензий для ОП AIC вариант «Стандартный»

BillManager	Лицензия на право установки и использования программного обеспечения BILL manager 6 редакции Enterprise, способ передачи электронный, сроком на 36 месяцев, с включенной технической поддержкой тип "Привилегированная" на 36 мес.	1	АО "ЭКЗОСОФТ"
	Лицензия на право установки и использования программного обеспечения BILL manager 6 редакции Enterprise, способ передачи электронный, сроком на 24 месяцев, с включенной технической поддержкой тип "Привилегированная" на 24 мес.	1	АО "ЭКЗОСОФТ"

7.4 Приложение 3. Документация по продуктам из состава AIC

7.4.1 Приложение 3.1 ПК СВ «Брест»

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

Руководство администратора Часть 1 (описан порядок развёртывания ПК СВ «Брест»).
Включает в себя разделы:

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

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

7.4.2 Приложение 3.2 ПО ALD Pro

Первичная настройка происходит по руководству администратора ALD Pro
Руководство администратора (описан порядок развёртывания комплекса)
Включает в себя разделы:

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

7.4.3 Приложение 3.1 ПО RuBackup

Руководство администратора (описан порядок развёртывания 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

7.4.4 Приложение 3.2 ОС СН Astra Linux

Документация на ОС СН Astra Linux

7.5 Приложение 4. Версии ПО в составе AIC

Табл.18. Версии ПО в составе AIC

Компонента AIC	Версия
ОС СН Astra Linux	1.7.2.UU1
ПК СВ ПК СВ «Брест»	3.2

Компонента AIC	Версия
Rubackup	2.0

7.6 Приложение 5. Совместимые гостевые ОС

Табл.19. Совместимые гостевые ОС

Семейство ОС	Версии
Astra Linux	1.3, 1.4, 1.5, 1.6, 1.7, 2.12
Windows	Win7, Win10, WinServ2008, WinServ2012, WinServ2016, WinServ2021
Linux	Debian 11, Ubuntu 22, Fedora 37

7.7 Приложение 6. API

Табл.20. API

Компонент	API
ПК СВ «Брест»	Opennebula XML-RPC Инструкции ПК СВ «Брест»
ALD Pro	Документ aldpro-api
RuBackup	Руководство по установке и взаимодействию с программным интерфейсом RuBackup REST API

7.8 Приложение 7. Минимальные[12] требования к ресурсам

Табл.21. Минимальные требования к ресурсам. Базовая конфигурация.

Базовая конфигурация		
Сервер 1	Сервер 2	Сервер 3
ALSE	ALSE	ALSE
ALD Pro	ALD Pro	RuBackup
ПК СВ «Брест»	ПК СВ «Брест»	ПК СВ «Брест»

Минимальные требования к ресурсам для каждого сервера бКОР: 18 ядер CPU и 32 ГБ RAM.

Табл.22. Минимальные требования к ресурсам. Стандартная конфигурация.

Стандартная конфигурация		
Сервер 1	Сервер 2	Сервер 3
ALSE	ALSE	ALSE
ALD Pro	ALD Pro	RuBackup
ПК СВ «Брест»	ПК СВ Брест	ПК СВ «Брест»
Astra Monitoring	DCImanager	BILLmanager
Astra Automation		

[12] В расчётах приведены данные без требований к программно-определяемой СХД. Расчёт приведён для тестовой среды.

Минимальные требования к ресурсам для каждого сервера бКОР: 32 ядра CPU и 64 ГБ RAM.

8 Список рисунков

9 Список таблиц

10 Термины и аббревиатуры

Табл.23. Термины и аббревиатуры

AFICK	«Another File Integrity Checker». утилита контроля целостности системы
ELF	Формат исполняемого файла
BD	Bridge Domain Interface — логический интерфейс, обеспечивающий двунаправленный трафик между сетью с мостовыми подключениями уровня 2 и сетью с маршрутизацией уровня 3.
iBGP	internal BGP является одной из форм протокола BGP для обмена информацией о маршрутах внутри AS. Border Gateway Protocol (BGP) — протокол динамической маршрутизации, относится к классу протоколов маршрутизации внешнего шлюза (EGP). На текущий момент является основным протоколом динамической маршрутизации в сети Интернет.
IPMI	IPMI (от англ. Intelligent Platform Management Interface) — интеллектуальный интерфейс управления платформой, предназначенный для автономного мониторинга и управления функциями, встроенными непосредственно в аппаратное и микропрограммное обеспечения серверных платформ. Ключевые характеристики IPMI — мониторинг, восстановление функций управления, журналирование и инвентаризация, которые доступны независимо от процессора, BIOS'а и операционной системы. Функции управления платформой могут быть доступны, даже если система находится в выключенном состоянии.
M-LAG	MLAG или MC-LAG означает агрегирование каналов мульти-шасси. Это технология агрегации каналов с несколькими устройствами, которая позволяет двум коммутаторам работать как один коммутатор. Порты от разных одноранговых коммутаторов MLAG объединяются в единый логический канал, обеспечивая увеличенную пропускную способность канала и дополнительную избыточность.
PARSEC	подсистема безопасности, использующая формальную модель разграничения доступа. Была разработана в Институте криптографии, связи и информатики Академии ФСБ России.
QEMU	программа с открытым исходным кодом для эмуляции аппаратного обеспечения различных платформ
RAFT	алгоритм для решения задач консенсуса в сети ненадёжных вычислений
RBD	RADOS Block Device – метод выделения пространства с Ceph и презентации его клиентам в виде блочных устройств (дисков).
SPICE	SPICE — протокол удаленного доступа к рабочему столу, ориентированный на использование в виртуальной среде. При разработке протокола особо учитывались требования, необходимые для работы с мультимедиа контентом. SPICE использует специальные кодеки для сжатия аудио и видео, что позволяет обеспечить двунаправленную передачу звука, а также возможность просмотра видео на удалённой машине.
VBDIF	Интерфейс, настраиваемый на шлюзе уровня 3 VXLAN, представляет собой логический интерфейс уровня 3, созданный на основе BD. Используя интерфейс VBDIF для настройки IP-адресов, VXLAN разных сегментов сети могут взаимодействовать с другими VXLAN и соединять сети уровня 2 с сетями уровня 3.
VLAN	Virtual Local Area Network — виртуальная локальная компьютерная сеть. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет устройствам группироваться вместе, даже если они не находятся в одной физической сети.
VNC	Virtual Network Computing (VNC) — система удалённого доступа к рабочему столу компьютера

VRRP	Virtual Router Redundancy Protocol — сетевой протокол, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию. Это достигается путём объединения группы маршрутизаторов в один виртуальный маршрутизатор и назначения им общего IP-адреса, который и будет использоваться как шлюз по умолчанию для компьютеров в сети.
VTEP	Vitual Tunnel End Point, устройство на котором начинается или заканчивается VxLAN тоннель. VTEP это не обязательно какое-либо сетевое устройство. Так же может выступать и сервер с поддержкой технологии VxLAN.
VxLAN	Virtual Extensible LAN является технологией сетевой виртуализации, созданной для решения проблем масштабируемости в больших системах облачных вычислений. VxLAN это протокол инкапсуляции, который обеспечивает подключение центров обработки данных с использованием туннелирования для расширения соединений уровня 2 (Ethernet кадров) в используемой сети уровня 3 (UDP-пакеты).
Zabbix	Система мониторинга статусов разнообразных сервисов компьютерной сети, серверов и сетевого оборудования. Для хранения данных используется MySQL, PostgreSQL, SQLite или Oracle Database, веб-интерфейс написан на PHP.
СХД	Система хранения данных
ПСХД	Программно-определяемая система хранения данных
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ПК	Программный комплекс
ОП	Облачная Платформа Astra Infrastructure Cloud
ОС СН	Служба доступа к сетевой защищённой файловой системе
МДЗ	Модуль доверенной загрузки представляет собой комплекс аппаратно-программных средств, устанавливаемый на рабочее место вычислительной системы (персональный компьютер, сервер, ноутбук, специализированный компьютер и др.).
СРК	Система резервного копирования
АСЗИ	Автоматизированная система в защищённом исполнении
БД	База данных
ВМ	Виртуальная машина
ЗПС	Замкнутая программная среда
КСПД	Корпоративная сеть передачи данных
ОС	Операционная система