КИБЕРПРОТЕКТ

КИБЕР
Бэкап Облачный

Версия 26.03

Развёртывание частного облака

Редакция: 20.04.2026

Содержание

Заявление об авторских правах

1 Введение

В данном руководстве описано развёртывание частного облака на основе Кибер Бэкапа Облачного в закрытом или открытом контуре.

2 Используемые константы

В настоящем документе используются следующие константы:

- <vdc> – полное имя виртуального ЦОД, предоставляемое ООО "Киберпротект" (например, nn01-cloud).
- <short_vdc> – краткое имя виртуального ЦОД, предоставляемое ООО "Киберпротект". Соответствует значению <vdc> без "-cloud", например, nn01.
- <pdc> – полное имя физического ЦОД, предоставляемое ООО "Киберпротект" (например, mos01).
- <internal_domain> – домен стенда (например, corplatform.ru).
- <NN> – номер кластера, может принимать значения:
  - 01 – если используется гибридная схема;
  - 02 – если шлюз Backup Gateway и хранилище резервных копий (т. н. "холодное" хранилище) выделены в отдельный кластер Кибер Инфраструктуры.

3 Рекомендуемая инфраструктура

Состав необходимой инфраструктуры частного облака на основе Кибер Бэкапа Облачного зависит от количества поддерживаемых агентов и учётных записей, а также от целевого объёма полезного места хранилища.

В документе "Проектирование и типовое развёртывание частного облака" приведены:

- сведения о базовой инфраструктуре,
- требования к подключению хранилищ резервных копий,
- рекомендации по масштабированию.

4 Сетевые соединения

Базовая конфигурация сетевых соединений серверов и кластеров, необходимых для развёртывания Кибер Бэкапа Облачного в частном облаке, зависит от используемого варианта:

- с отдельными кластерами вычислений и хранения резервных копий (рекомендуемый вариант для промышленной эксплуатации);
- с гибридным кластером, совмещающим функции вычислений и хранения резервных копий.

Соответствующие схемы сетевых соединений приведены на рисунках ниже.

Схема для варианта с отдельными кластерами вычислений и хранения резервных копий

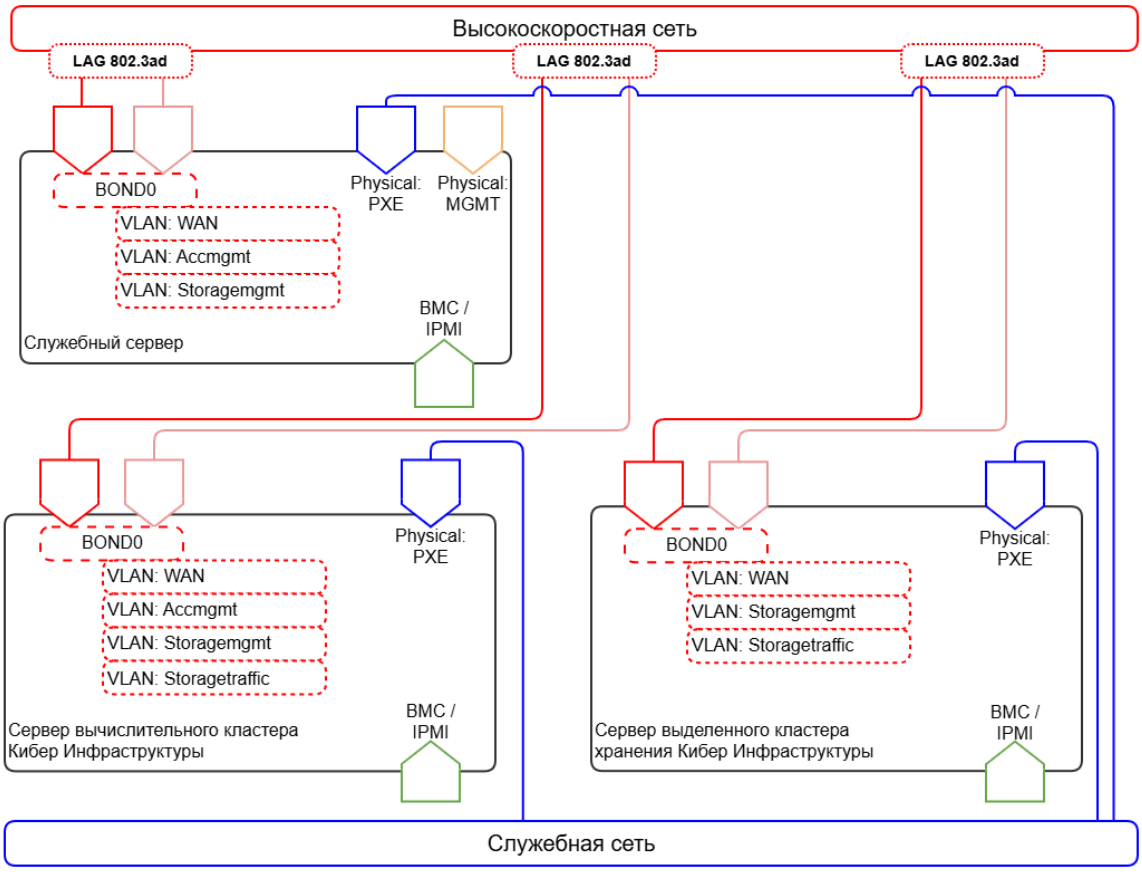
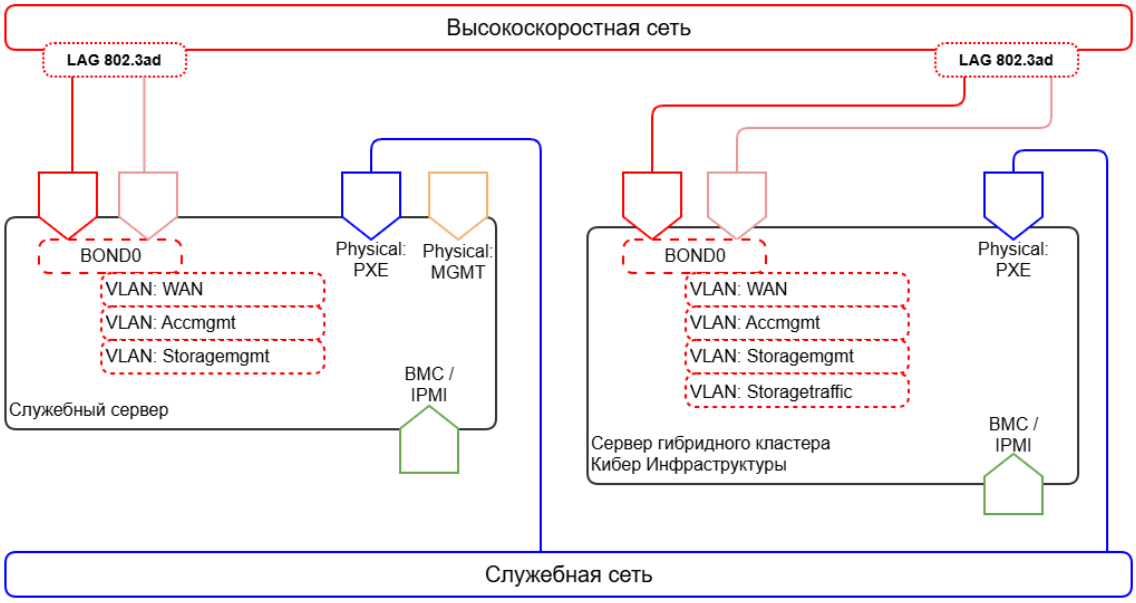


Схема для варианта с гибридным кластером



Описание обозначенных на рисунках элементов схем приведено далее.

4.1 Сети

- **Высокоскоростная сеть** – сеть, предназначенная для передачи данных между Кибер Инфраструктурой и Кибер Бэкапом Облачным на высокой скорости (от 10 Гб/с и выше) с минимальными задержками (до 100 мкс).
- **Служебная сеть** – сеть, предназначенная для установки и развёртывания служебного сервера, Кибер Инфраструктуры и других компонентов стенда, а также для управления Кибер Инфраструктурой и служебным сервером при сбоях высокоскоростной сети.

4.2 Серверы

- **Служебный сервер** – сервер, предназначенный для размещения служб, необходимых для автоматизации процессов подготовки Кибер Инфраструктуры и Кибер Бэкапа Облачного, хранения данных, используемых в процессах автоматизации, а также для маршрутизации трафика между сетями стенда и других инфраструктурных задач.
- **Сервер вычислительного кластера** – сервер кластера Кибер Инфраструктуры, в котором разворачивается вычислительный кластер (средства виртуализации) и не разворачивается шлюз Backup Gateway.
- **Сервер кластера хранения** – сервер кластера Кибер Инфраструктуры, в котором разворачивается только шлюз Backup Gateway.
- **Сервер гибридного кластера** – сервер кластера Кибер Инфраструктуры, в котором разворачивается и вычислительный кластер (средства виртуализации), и шлюз Backup Gateway.

Примечание
Для эксплуатации в промышленных условиях рекомендуется использовать отдельные кластеры для вычислений и хранения резервных копий вместо гибридного кластера.

4.3 Интерфейсы

- **LAG 802.3ad** – объединение физических портов в режиме "Активный-Активный" на сетевом оборудовании. Параметры объединения:
  - miimon=100;
  - mode=802.3ad;
  - lacp_rate=fast;
  - xmit_hash_policy=layer2+3.
- **Bond0** – группа объединённых физических портов в режиме "Активный-Активный" в Linux-подобных операционных системах. Параметры объединения:
  - miimon=100;
  - mode=802.3ad;
  - lacp_rate=fast;
  - xmit_hash_policy=layer2+3.

Примечание
Для промышленной эксплуатации стенда в группы объединённых физических портов **LAG 802.3ad** и **Bond0** должно быть включено не менее двух физических портов. Включение в вышеуказанные группы по одному физическому порту допустимо только для тестовых и аналогичных сред.

- **VLAN: WAN** – развёрнутый поверх группового интерфейса **bond0** виртуальный интерфейс в выделенной сети **WAN**. Данная сеть является маршрутизируемой и предназначена для взаимодействия агентов резервного копирования и пользователей веб-консоли с Кибер Бэкапом Облачным.

  В сети **WAN** назначаются IP-адреса:
  - служб, принимающих внешние подключения;
  - шлюза Backup Gateway;
  - внутреннего репозитория;
  - служебного сервера.

  Для сети **WAN** требуется не менее 30 доступных IP-адресов, не включая служебные (сеть с префиксом 27).
- **VLAN: Accmgmt** – развёрнутый поверх группового интерфейса **bond0** виртуальный интерфейс в выделенной сети **Accmgmt**. Данная сеть предназначена для взаимодействия виртуальных машин Кибер Бэкапа Облачного.

Сеть **Accmgmt** может быть маршрутизируемой для обеспечения прямого доступа из внутренних сетей к виртуальным машинам Кибер Бэкапа Облачного (например, для обслуживания и диагностики при сбоях). Маршрутизация для данной сети не является обязательной.

Для сети **Accmgmt** требуется не менее 254 доступных IP-адресов, не включая служебные (сеть с префиксом 24).

- **VLAN: Storagemgmt** – развёрнутый поверх группового интерфейса **bond0** виртуальный интерфейс в выделенной сети **Storagemgmt**. Данная сеть предназначена для взаимодействия управляющих служб кластера Кибер Инфраструктуры (в том числе компонентов управления шлюза Backup Gateway).

  Сеть **Storagemgmt** может быть маршрутизируемой для обеспечения прямого доступа из внутренних сетей к виртуальным машинам Кибер Бэкапа Облачного (например, для обслуживания и диагностики при сбоях). Маршрутизация для данной сети не является обязательной.

  Для сети **Storagemgmt** требуется не менее 254 доступных IP-адресов, не включая служебные (сеть с префиксом 24).
- **VLAN: Storagetraffic** – развёрнутый поверх группового интерфейса **bond0** виртуальный интерфейс в выделенной сети **Storagetraffic**. Данная сеть предназначена только для внутреннего трафика программно определяемого хранилища (SDS) Кибер Инфраструктуры.

  Примечание
  Интерфейсы в сети **Storagetraffic** настраиваются только на серверах Кибер Инфраструктуры и не настраиваются на служебных серверах.

  Сеть **Storagetraffic** не должна быть маршрутизируемой.

  Для данной сети требуется не менее 254 доступных IP-адресов, не включая служебные (сеть с префиксом 24).

  Примечание
  Количество IP-адресов в сети **Storagetraffic** должно соответствовать количеству IP-адресов в сети **Storagemgmt**.

- **Physical: PXE** – физический интерфейс в выделенной сети **PXE**. Данная сеть предназначена для первичной установки и настройки служебных серверов и серверов Кибер Инфраструктуры.

  Сеть **PXE** может быть маршрутизируемой для обеспечения резервного прямого доступа из внутренних сетей к служебному серверу и серверам Кибер Инфраструктуры. Маршрутизация для данной сети не является обязательной.

  Для данной сети требуется не менее 254 доступных IP-адресов, не включая служебные (сеть с префиксом 24).
- **Physical: MGMT** – физический интерфейс в выделенной сети **MGMT**. Данная сеть используется для подключения к служебному серверу до запуска его автоматической настройки. IP-конфигурация интерфейса **MGMT** может быть получена как через внутренний DHCP-сервер эксплуатирующей организации, так и настроена вручную. Системное наименование данного интерфейса указывается в качестве резервного при заполнении формы первичных настроек

стенда.

Интерфейс сети **MGMT** может быть заменён аналогичным интерфейсом в сети **PXE**. В этом случае при заполнении формы первичных настроек стенда укажите системное наименование интерфейса **PXE** в качестве резервного и вручную настройте его IP-конфигурацию.

Примечание

В этой сети интерфейсы настраиваются только на служебных серверах; настройка интерфейсов на серверах Кибер Инфраструктуры не предусмотрена.

- **BMC/IPMI** – интерфейсы серверов для удалённого управления, настраиваются эксплуатирующей организацией. Средства автоматизации установки и настройки служебного сервера, Кибер Инфраструктуры и Кибер Бэкапа Облачного для стендов частного облака не используют эти интерфейсы.

5 Развёртывание частного облака на основе Кибер Бэкапа Облачного

Процесс развёртывания частного облака на основе Кибер Бэкапа Облачного включает в себя:

- подготовку SSL-сертификатов;
- создание DNS-записей;
- установку служебного сервера;
- подготовку конфигурации стенда;
- копирование файлов на служебный сервер;
- формирование переменных и других обязательных элементов стенда;
- настройку служебного сервера;
- настройку вычислительного (гибридного) кластера;
- настройку кластера хранения резервных копий (при его наличии);
- настройку внутреннего репозитория и служебных виртуальных машин;
- получение дистрибутивов агентов резервного копирования;
- установку Кибер Бэкапа Облачного.

Подробные инструкции для каждого этапа приведены в соответствующих разделах настоящего документа.

5.1 Подготовка SSL-сертификатов

Подготовьте SSL-сертификаты для следующих доменных имён:

- infra-jenkins-<pdc>.<internal_domain>;
- cloud-jenkins-<short_vdc>.<internal_domain>;
- <vdc>.<internal_domain>;
- rs-<vdc>.<internal_domain>;
- cloud-wr-<short_vdc>.<internal_domain>;
- agents-<vdc>.<internal_domain>;
- <pdc>-repo.<internal_domain>.

Примечание
Доменные имена infra-jenkins-<pdc>.<internal_domain> и cloud-jenkins-<short_vdc>.<internal_domain> должны быть указаны в отдельном общем SSL-сертификате. Остальные доменные имена могут быть указаны как в одиночных сертификатах (Single Domain), так и в одном или нескольких сертификатах с подстановочным знаком (Wildcard) или в мультидоменных SSL-сертификатах (SAN).

5.2 Создание DNS-записей

Для корректного функционирования стенда создайте DNS-записи на внутренних DNS-серверах, отвечающих за домен.

5.2.1 Используемые IP-адреса

При создании DNS-записи требуется указать IP-адрес, соответствующий доменному имени. Для ряда доменных имён в таблице ниже приведены индексы соответствующих IP-адресов.

Индекс IP-адреса в маршрутизируемой сети (WAN) – это порядковый номер IP-адреса, используемого при создании DNS-записи, в выделенном сегменте маршрутизируемой сети (WAN). Нумерация индексов начинается с 0.

Например, в подсети 100.10.10.128/27:

- IP-адрес 100.10.10.128 имеет индекс 0;
- IP-адрес 100.10.10.129 имеет индекс 1;
- IP-адрес 100.10.10.130 имеет индекс 2 и так далее.

Последние два IP-адреса из выделенного сегмента сети (кроме служебного IP-адреса для широковещательной рассылки) используются для специальных компонентов Кибер Бэкапа Облачного, для которых не требуется настройка DNS-записей. Так, в подсети 100.10.10.128/27 из примера выше:

- IP-адрес 100.10.10.157 с индексом 29 и IP-адрес 100.10.10.158 с индексом 30 используются для специальных компонентов Кибер Бэкапа Облачного, не требующих настройки DNS-записей;
- IP-адрес 100.10.10.159 с индексом 31 – служебный IP-адрес для широковещательной рассылки.

Незадействованные IP-адреса выделенного сегмента маршрутизируемой сети (при их наличии) резервируются для дальнейшего масштабирования кластера Кибер Инфраструктуры с развёрнутым шлюзом Backup Gateway и для подключения новых служб.

Примечание
Если в выделенном сегменте маршрутизируемой сети часть IP-адресов занята, а их индексы соответствуют указанным в таблице, то при настройке DNS-записей укажите свободные индексы в том же количестве и передайте эту информацию ООО "Киберпротект" для дальнейшей корректировки переменной, отвечающей за распределение IP-адресов.

5.2.2 Настройка DNS-записей

На внутренних DNS-серверах создайте DNS-записи для доменных имён в соответствии с таблицей.

DNS-имя	Тип DNS-записи	Индекс IP-адреса в маршрутизируемой сети (WAN)	Целевое имя
<vdc>.<internal_domain>	A	6, 7	-
rs-<vdc>.<internal_domain>	CNAME	-	<vdc>.<internal_domain>
cloud-wr-<short_vdc>.<internal_domain>	CNAME	-	<vdc>.<internal_domain>
agents-<vdc>.<internal_domain>	A	8, 9	-
<pdc>-repo.<internal_domain>	A	10	-
cloud-jenkins-<short_vdc>.<internal_domain>	A	4, 5	-
infra-jenkins-<pdc>.<internal_domain>	CNAME	-	cloud-jenkins-<short_vdc>.<internal_domain>
abgw-<pdc>-aci<NN>.<internal_domain>	A	С 11 по <X> включительно	-

В этой таблице:

- <X> – индекс IP-адреса в маршрутизируемой сети (WAN), определяемый по формуле:

  <X> = 10 + <N>

  В этом выражении:

  - <N> – количество узлов кластера Кибер Инфраструктуры, где развёрнуты шлюз Backup Gateway и хранилище резервных копий.

Пример

В таблице ниже приведён пример для следующих значений:

- полное имя виртуального ЦОД (<vdc>) – nn01-cloud;
- краткое имя виртуального ЦОД (<short_vdc>) – nn01;
- полное имя физического ЦОД (<pdc>) – mos01;
- домен стенда (<internal_domain>) – corplatform.ru;
- номер кластера (<NN>) – "02" (шлюз Backup Gateway и хранилище резервных копий выделены в отдельный кластер Кибер Инфраструктуры);
- <X> – 15;
- используемая подсеть – 100.10.10.128/27.

DNS-имя	Тип DNS-записи	Индекс IP-адреса в маршрутизируемой сети (WAN)	Целевое имя
nn01-cloud.corplatform.ru	A	6, 7	-
rs-nn01-cloud.corplatform.ru	CNAME	-	nn01-cloud.corplatform.ru
cloud-wr-nn01.corplatform.ru	CNAME	-	nn01-cloud.corplatform.ru
agents-nn01-cloud.corplatform.ru	A	8, 9	-
mos01-repo.corplatform.ru	A	10	-
cloud-jenkins-nn01.corplatform.ru	A	4, 5	-
infra-jenkins-mos01.corplatform.ru	CNAME	-	cloud-jenkins-nn01.corplatform.ru
abgw-mos01-aci02.corplatform.ru	A	С 11 по 15 включительно	-

5.3 Установка служебного сервера

Выполните следующие шаги:

1. Подготовьте USB-накопитель, записав на него полученный от ООО "Киберпротект" образ ISO. Способ получения образа ISO определяется индивидуально (например, может быть предоставлена ссылка для скачивания ISO-образа).
2. Загрузите служебный сервер с использованием подготовленного USB-накопителя.
3. Установите систему в автоматическом режиме.
4. По завершении установки дождитесь выключения сервера и извлеките из него USB-накопитель. После этого включите сервер вновь.
5. Войдите на служебный сервер с использованием интерфейса BMC/IPMI (или напрямую, подключив к нему монитор и клавиатуру).
6. Настройте IP-адрес и маску подсети, а также прочие параметры для интерфейса MGMT (или интерфейса PXE при его использовании вместо MGMT). Он будет использоваться только до завершения настройки параметров сети служебного сервера.
7. Подключитесь к служебному серверу по SSH, используя настроенный на предыдущем шаге IP-адрес интерфейса MGMT (или интерфейса PXE).
8. Убедитесь, что система SELinux отключена в конфигурации и фактически:

```
# sestatus
# grep -x SELINUX /etc/selinux/config
```

Если система SELinux не отключена в конфигурации, установите значение SELINUX=disabled. Если текущее значение SELINUX не "disabled", перезагрузите служебный сервер.

9. Скопируйте на служебный сервер SSL-сертификат и ключ сертификата для хостов infra-jenkins-<short_vdc>.<internal_domain> и cloud-jenkins-<short_vdc>.<internal_domain>.

Внимание
На текущий момент автоматически можно добавить только один сертификат для двух доменных имён хостов Jenkins. Используйте Wildcard-сертификат или Alternative DNS Names при подготовке сертификата.

10. Запустите скрипт первоначальной настройки:

```
/opt/client-artifacts/docker/docker_container_manage.sh -c <путь_к_файлу_сертификата> -k <путь_к_файлу_закрытого_ключа>
```

В этом выражении:

- <путь_к_файлу_сертификата> – полный путь к файлу сертификата;
- <путь_к_файлу_закрытого_ключа> – полный путь к файлу закрытого ключа сертификата.

Скрипт отобразит пароли пользователя admin для серверов infra-jenkins и cloud-jenkins. Сохраните их, они потребуются для входа в веб-интерфейс Jenkins.

Примечание
После первой аутентификации средствами Jenkins можно изменить пароль администратора, а также добавить новых пользователей. Подробнее см. в документации Jenkins.

11. Убедитесь в отсутствии ошибок в выводе скрипта и перейдите к формированию конфигурации стенда. Если возникли ошибки, устраните их причину перед продолжением.

5.4 Формирование конфигурации стенда

Настройте конфигурацию стенда, выполнив следующие действия:

1. Откройте веб-форму ввода параметров конфигурации стенда по адресу https://cloud-jenkins-<short_vdc>.<internal_domain>/fp
2. На вкладке **Общие параметры** последовательно раскройте разделы настроек, нажав на их заголовки. Заполните обязательные поля (отмечены символом "*"), введя значение вручную или выбрав его из выпадающего списка.
3. На вкладке **Конфигурация пользователей** заполните параметры для пользователя, указав значение в обязательных полях (отмечены символом "*").
4. [Необязательно] Для добавления нового пользователя щёлкните **Добавить пользователя** и заполните его параметры.

5. [Необязательно] Для удаления пользователя нажмите **Удалить пользователя**.
6. Нажмите кнопку **Сгенерировать JSON**. Если какой-то обязательный параметр не был заполнен или был заполнен неверно, рядом с соответствующим полем отобразится подсказка.
7. Щёлкните **Сохранить JSON в файл** и сохраните сгенерированный JSON-файл. Он потребуется для формирования переменных на дальнейших этапах установки.

5.5 Копирование файлов на служебный сервер

Скопируйте файлы на служебный сервер, выполнив следующие действия:

1. Получите у специалистов ООО "Киберпротект" ссылку на каталог, содержащий все файлы, необходимые для копирования на служебный сервер.
2. Подключитесь к служебному серверу по SSH, используя IP-адрес интерфейса MGMT (или интерфейса PXE, если он применяется вместо MGMT).
3. На служебном сервере создайте директории для копирования файлов:

   ```
   mkdir -p <sep_artefacts_dir>/templates/kvm
   ```

   В этой команде:

   - <sep_artefacts_dir> – значение параметра **Каталог образов** веб-формы, заполненной на шаге "Формирование конфигурации стенда" (стр. 16).

     Рекомендованное значение параметра – /opt/client-artifacts/separts.

     Пример полной команды:

     ```
     mkdir -p /opt/client-artifacts/separts/templates/kvm
     ```

     Внимание
     Значения первых двух частей пути (/opt/client-artifacts) и последних двух частей пути (/templates/kvm) менять нельзя.

4. Загрузите все файлы образов виртуальных машин, используя полученную от специалистов ООО "Киберпротект" ссылку, в папку <sep_artefacts_dir>/templates/kvm.

   Пример команд для случая двух файлов образов виртуальных машин:

   ```
   curl -o /opt/client-artifacts/separts/templates/kvm/redos-template
   https://pdl.cyberprotect.ru/20087c2a-ced6-48b3-b0b8-cf426182e2b9/templates/kvm/redos-
   template
   curl -o /opt/client-artifacts/separts/templates/kvm/repo-template
   https://pdl.cyberprotect.ru/20087c2a-ced6-48b3-b0b8-cf426182e2b9/templates/kvm/repo-
   template
   ```

   Вместо использованного в примере выше ресурса https://pdl.cyberprotect.ru/20087c2a-ced6-48b3-b0b8-cf426182e2b9 должен быть использован другой промежуточный ресурс или внешний носитель.

5. Загрузите все остальные файлы образов, используя полученную от специалистов ООО "Киберпротект" ссылку, в папку <sep_artefacts_dir>.

   Пример команды для обычного набора файлов:

   ```
   curl -o /opt/client-artifacts/separts/cyber-infrastructure-5.5.1.iso
   https://pdl.cyberprotect.ru/20087c2a-ced6-48b3-b0b8-cf426182e2b9/cyber-infrastructure-
   5.5.1.iso
   curl -o /opt/client-artifacts/separts/cyber-infrastructure-5.5.1.iso.checksum
   https://pdl.cyberprotect.ru/20087c2a-ced6-48b3-b0b8-cf426182e2b9/cyber-infrastructure-
   5.5.1.iso.checksum
   curl -o /opt/client-artifacts/separts/redos-MUROM-7.3.5-20241106.3-Everything-x86_64-
   DVD1.iso https://pdl.cyberprotect.ru/20087c2a-ced6-48b3-b0b8-cf426182e2b9/redos-MUROM-
   7.3.5-20241106.3-Everything-x86_64-DVD1.iso
   curl -o /opt/client-artifacts/separts/redos-MUROM-7.3.5-20241106.3-Everything-x86_64-
   DVD1.iso.checksum https://pdl.cyberprotect.ru/20087c2a-ced6-48b3-b0b8-
   cf426182e2b9/redos-MUROM-7.3.5-20241106.3-Everything-x86_64-DVD1.iso.checksum
   ```

   Вместо использованного в примере выше ресурса https://pdl.cyberprotect.ru/20087c2a-ced6-48b3-b0b8-cf426182e2b9 должен быть использован другой промежуточный ресурс или внешний носитель.

5.6 Формирование переменных и других обязательных элементов стенда

Предупреждение
Данный этап не является идемпотентным: каждый повторный запуск приводит к перезаписи существующих файлов (переменных, сертификатов и др.). Перед внесением изменений система автоматически создает резервную копию каталогов.

Для формирования переменных и других обязательных элементов стенда выполните следующие действия:

1. Откройте веб-интерфейс Jenkins по адресу https://cloud-jenkins-<short_vdc>.<internal_domain>.
2. Откройте сборку **abc_prepare_enclosed_basics_minparams_trigger**, выбрав её в общем списке на главной панели. Для поиска воспользуйтесь строкой поиска в верхней части страницы.
3. Нажмите **Собрать с параметрами**.
4. Укажите параметры сборки:
   - **customer_params** – вставьте текст, скопированый из JSON-файла, сформированного на предыдущем этапе.
   - **BUILD_VERSION** – укажите актуальную версию Кибер Бэкапа Облачного (при необходимости уточните её номер в ООО "Киберпротект").
   - **environment_dir** – оставьте значение по умолчанию production-deployment-environments.
   - **EXTRA_VARS** – оставьте поле пустым.

- **JIRA_TASK_ID** – при настроенной интеграции с Jira введите идентификатор задачи, в противном случае оставьте поле пустым.

5. Нажмите **Собрать**.
6. [Рекомендуется] После начала сборки перейдите в режим **Blue Ocean**. Для этого в столбце **История сборок** откройте активную сборку, затем в окне сборки щёлкните **Open Blue Ocean**.
7. При запросе введите в соответствующее поле пароль учётной записи для отправки email-сообщений.
8. При запросе SSL-сертификатов хостов и закрытых ключей скопируйте их содержимое из соответствующих файлов и вставьте в требуемые поля.

   Количество запрашиваемых данных зависит от типа сертификата, выбранного на этапе заполнения веб-формы: это будет либо один запрос для Wildcard-сертификата, либо отдельные запросы для каждого компонента стенда, требующего публичного DNS-имени.
9. При запросе цепочки сертификатов скопируйте содержимое промежуточного и корневого сертификатов в соответствующие поля. Если сертификаты хостов содержат эту информацию, оставьте данные поля пустыми.
10. Дождитесь завершения сборки.

5.7 Настройка служебного сервера

Для настройки служебного сервера выполните следующие действия:

1. Откройте веб-интерфейс Jenkins по адресу https://cloud-jenkins-<short_vdc>.<internal_domain>.
2. Откройте сборку **abc_deploy_side_server_trigger**, выбрав её в общем списке на главной панели. Для поиска воспользуйтесь строкой поиска в верхней части страницы.
3. Нажмите **Собрать с параметрами**.
4. Укажите параметры сборки:
   - **BUILD_VERSION** – укажите актуальную версию Кибер Бэкапа Облачного (при необходимости уточните её номер в ООО "Киберпротект").
   - **EXTRA_VARS** – оставьте поле пустым.
   - **JIRA_TASK_ID** – при настроенной интеграции с Jira введите идентификатор задачи, в противном случае оставьте поле пустым.
5. Нажмите **Собрать**.
6. [Рекомендуется] После начала сборки перейдите в режим **Blue Ocean**. Для этого в столбце **История сборок** откройте активную сборку, затем в окне сборки щёлкните **Open Blue Ocean**.
7. Если для вычислений и резервного копирования предусмотрены отдельные кластеры, укажите инвентарь вычислительного кластера ***aci01**.

   Примечание
   При использовании гибридного кластера, совмещающего функции вычисления и хранения резервных копий, этап выбора инвентаря будет пропущен.

8. Дождитесь завершения сборки.

5.8 Настройка вычислительного (гибридного) кластера

Для настройки вычислительного кластера (или гибридного кластера при его использовании) выполните следующие действия:

1. Откройте веб-интерфейс Jenkins по адресу https://cloud-jenkins-<short_vdc>.<internal_domain>.
2. Откройте сборку **abc_deploy_cyber_infra_cluster_trigger**, выбрав её в общем списке на главной панели. Для поиска воспользуйтесь строкой поиска в верхней части страницы.
3. Нажмите **Собрать с параметрами**.
4. Укажите параметры сборки:
   - **BUILD_VERSION** – укажите актуальную версию Кибер Бэкапа Облачного (при необходимости уточните её номер в ООО "Киберпротект").
   - **EXTRA_VARS** – оставьте поле пустым.
   - **JIRA_TASK_ID** – при настроенной интеграции с Jira введите идентификатор задачи, в противном случае оставьте поле пустым.
5. Нажмите **Собрать**.
6. [Рекомендуется] После начала сборки перейдите в режим **Blue Ocean**. Для этого в столбце **История сборок** откройте активную сборку, затем в окне сборки щёлкните **Open Blue Ocean**.
7. Если для вычислений и резервного копирования предусмотрены отдельные кластеры, укажите инвентарь вычислительного кластера ***aci01**.

   Примечание
   При использовании гибридного кластера, совмещающего функции вычисления и хранения резервных копий, этап выбора инвентаря будет пропущен.

8. Дождитесь завершения сборки.

5.9 Настройка кластера хранения резервных копий

Примечание
Данный этап актуален только для стендов с выделенными кластерами хранения и вычислений. Если на стенде развёрнут гибридный кластер, настройка не требуется.

Для настройки кластера хранения резервных копий выполните следующие действия:

1. Откройте веб-интерфейс Jenkins по адресу https://cloud-jenkins-<short_vdc>.<internal_domain>.
2. Откройте сборку **abc_deploy_cyber_infra_storage_cluster_trigger**, выбрав её в общем списке на главной панели. Для поиска воспользуйтесь строкой поиска в верхней части страницы.
3. Нажмите **Собрать с параметрами**.
4. Укажите параметры сборки:

- **BUILD_VERSION** – укажите актуальную версию Кибер Бэкапа Облачного (при необходимости уточните её номер в ООО "Киберпротект").
- **EXTRA_VARS** – оставьте поле пустым.
- **JIRA_TASK_ID** – при настроенной интеграции с Jira введите идентификатор задачи, в противном случае оставьте поле пустым.

5. Нажмите **Собрать**.
6. [Рекомендуется] После начала сборки перейдите в режим **Blue Ocean**. Для этого в столбце **История сборок** откройте активную сборку, затем в окне сборки щёлкните **Open Blue Ocean**.
7. Укажите инвентарь кластера хранения резервных копий ***aci02**.
8. Дождитесь завершения сборки.

5.10 Настройка внутреннего репозитория и служебных виртуальных машин

Для настройки внутреннего репозитория и служебных виртуальных машин выполните следующие действия:

1. Откройте веб-интерфейс Jenkins по адресу https://cloud-jenkins-<short_vdc>.<internal_domain>.
2. Откройте сборку **abc_deploy_abc_infra_vms_trigger**, выбрав её в общем списке на главной панели. Для поиска воспользуйтесь строкой поиска в верхней части страницы.
3. Нажмите **Собрать с параметрами**.
4. Укажите параметры сборки:
   - **BUILD_VERSION** – укажите актуальную версию Кибер Бэкапа Облачного (при необходимости уточните её номер в ООО "Киберпротект").
   - **EXTRA_VARS** – оставьте поле пустым.
   - **JIRA_TASK_ID** – при настроенной интеграции с Jira введите идентификатор задачи, в противном случае оставьте поле пустым.
5. Нажмите **Собрать**.
6. [Рекомендуется] После начала сборки перейдите в режим **Blue Ocean**. Для этого в столбце **История сборок** откройте активную сборку, затем в окне сборки щёлкните **Open Blue Ocean**.
7. Дождитесь завершения сборки.
8. Сообщите ООО "Киберпротект" о готовности внутреннего репозитория для начала его синхронизации.

5.11 Получение дистрибутивов агентов резервного копирования

Для загрузки дистрибутивов агентов в локальные каталоги и настройки ряда служебных компонентов продукта выполните следующие действия:

1. Откройте веб-интерфейс Jenkins по адресу https://cloud-jenkins-<short_vdc>.<internal_domain>.
2. Откройте сборку **abc_run_custom_playbook_trigger**, выбрав её в общем списке на главной панели. Для поиска воспользуйтесь строкой поиска в верхней части страницы.
3. Нажмите **Собрать с параметрами**.
4. Укажите параметры сборки:
   - **LOCK_INVENTORY** – рекомендуется снять флажок, блокировка инвентаря не позволит выполнить одновременно другую сборку с тем же инвентарём.
   - **BUILD_VERSION** – укажите актуальную версию Кибер Бэкапа Облачного (при необходимости уточните её номер в ООО "Киберпротект").
   - **PLAYBOOK_NAME** – укажите значение playbook-enclosed-agents.yml.
   - **EXTRA_VARS** – оставьте поле пустым.
   - **JIRA_TASK_ID** – при настроенной интеграции с Jira введите идентификатор задачи, в противном случае оставьте поле пустым.
5. Нажмите **Собрать**.
6. [Рекомендуется] После начала сборки перейдите в режим **Blue Ocean**. Для этого в столбце **История сборок** откройте активную сборку, затем в окне сборки щёлкните **Open Blue Ocean**.
7. При запросе инвентаря укажите инвентарь, путь к файлу которого заканчивается на ***-abc-infra**. Выбор другого инвентаря может привести к ошибкам и неверной настройке виртуальных машин.
8. Проверьте введённые параметры и подтвердите продолжение сборки.
9. Дождитесь завершения сборки.

5.12 Установка Кибер Бэкапа Облачного

Примечание
Установку Кибер Бэкапа Облачного можно начинать только после синхронизации репозитория. Убедитесь, что завершение этой операции подтверждено специалистами ООО "Киберпротект".

Для установки Кибер Бэкапа Облачного выполните следующие действия:

1. Откройте веб-интерфейс Jenkins по адресу https://cloud-jenkins-<short_vdc>.<internal_domain>.
2. Откройте сборку **abc_clean_install_trigger**, выбрав её в общем списке на главной панели. Для поиска воспользуйтесь строкой поиска в верхней части страницы.
3. Нажмите **Собрать с параметрами**.
4. Укажите параметры сборки:
   - **LOCK_INVENTORY** – рекомендуется снять флажок, блокировка инвентаря не позволит выполнить одновременно другую сборку с тем же инвентарём.
   - **BUILD_VERSION** – укажите актуальную версию Кибер Бэкапа Облачного (при необходимости уточните её номер в ООО "Киберпротект").
   - **EXTRA_VARS** – оставьте поле пустым.

- **JIRA_TASK_ID** – при настроенной интеграции с Jira введите идентификатор задачи, в противном случае оставьте поле пустым.

5. Нажмите **Собрать**.
6. [Рекомендуется] После начала сборки перейдите в режим **Blue Ocean**. Для этого в столбце **История сборок** откройте активную сборку, затем в окне сборки щёлкните **Open Blue Ocean**.
7. При запросе инвентаря укажите инвентарь, путь к файлу которого заканчивается на ***-cloud**. Выбор другого инвентаря может привести к ошибкам и неверной настройке виртуальных машин.
8. Проверьте введённые параметры и подтвердите продолжение сборки.
9. Дождитесь завершения сборки.

6 Проверка установки

Выполните следующие шаги:

1. Войдите в веб-интерфейс сервера cloud-jenkins по адресу https://cloud-jenkins-<short_vdc>.<internal_domain>. Для авторизации используйте имя учётной записи **admin** и пароль для cloud-jenkins, сгенерированный скриптом первоначальной настройки (см. раздел "Установка служебного сервера" (стр. 15)).
2. Откройте сборку **abc_clean_install_trigger**, выбрав её в общем списке на главной панели. Для поиска воспользуйтесь строкой поиска в верхней части страницы.
3. Нажмите **Open Blue Ocean**.
4. Выберите номер прогона в разделе **Build History** и убедитесь в том, что все стадии и шаги выделены зелёным цветом.
5. Перейдите по адресу http://<consul_ip>:8500/ui и убедитесь в отсутствии сервисов, имеющих состояние "Critical".

   Примечание
   - Значение <consul_ip> находится в каталоге служебного сервера /opt/client-artifacts/git/production-deployment-environments/progress_inventories/production/<vdc> в группе **Consul**.
   - Виртуальные машины службы **Consul** находятся в сети **Accmgmt** (подробнее см. в разделе "Сетевые соединения" (стр. 7)).

6. Перейдите по адресу http://<prometheus_ip>:9093/#/alerts и убедитесь в отсутствии активных сообщений, имеющих состояние "Critical" и "Disaster".

   Примечание
   - Значение <prometheus_ip> находится в каталоге служебного сервера /opt/client-artifacts/git/production-deployment-environments/progress_inventories/production/<vdc> в группе **Prometheus**.
   - Виртуальные машины службы **Prometheus** находятся в сети **Accmgmt** (подробнее см. в разделе "Сетевые соединения" (стр. 7)).

7 Настройка исключений для антивирусного ПО

В случае использования на сервере репозитория и служебном сервере антивирусных продуктов "Лаборатории Касперского" настройте исключения:

- Для сервера репозитория K8s-repo

  ```
  /home/syncthing
  /data
  ```

- Для служебного сервера cyberdc_gw

  ```
  /opt/client-artifacts/
  /var/ftp/iso
  /var/lib/dcm_common/
  ```

Примечание

Установка антивирусного ПО на другие компоненты решения не поддерживается.

8 Обновление

Процедура обновления состоит из двух частей:

- Обновления RPM-пакетов и образов контейнеров в репозитории.
- Обновления Ansible-плейбуков и Ansible-ролей на служебном сервере.

Способ получения компонентов обновления определяется индивидуально.

После получения компонентов обновления выполните следующие шаги:

1. Войдите в веб-интерфейс сервера cloud-jenkins по адресу https://cloud-jenkins-<short_vdc>.<internal_domain>. Для авторизации используйте имя учётной записи **admin** и пароль для cloud-jenkins, сгенерированный скриптом первоначальной настройки (см. раздел "Установка служебного сервера" (стр. 15)).
2. Откройте сборку **abc_tr_rollout_trigger**, выбрав её в общем списке на главной панели. Для поиска воспользуйтесь строкой поиска в верхней части страницы.
3. Нажмите **Собрать с параметрами**.
4. Для параметра **BUILD_VERSION** укажите актуальную версию Кибер Бэкапа Облачного (при необходимости уточните её номер в ООО "Киберпротект").
5. Нажмите **Собрать**.
6. Выберите файл inventory: <vdc>-cloud.
7. Выберите номер технического релиза и нажмите **Proceed**.
8. Дождитесь окончания процесса и выполните проверку установки (см. раздел "Проверка установки" (стр. 24)).

9 Развёртывание LDAP-коннектора

Для развёртывания LDAP-коннектора выполните следующие действия:

1. Средствами Кибер Инфраструктуры создайте виртуальную машину, используя шаблон РЕД ОС (подробнее см. в Руководстве администратора Кибер Инфраструктуры).
2. Установите LDAP-коннектор (подробнее см. в Руководстве администратора компании).

Количество развёрнутых LDAP-коннекторов должно соответствовать количеству тенантов типа **Клиент**.

Указатель