WHITE PAPER

РЕКОМЕНДАЦИИ ПО ОПТИМИЗАЦИИ И ИНТЕГРАЦИИ TATLIN.BACKUP.M С VEEAM BACKUP & REPLICATION V12.1

О WHITE PAPERS

Данный документ описывает архитектурные принципы и подходы, а также рекомендации по их применению при построении корпоративных решений на основе продуктов производства компании YADRO.

Документ предназначен для широкой аудитории, но также может включать материалы, требующие специальной профессиональной подготовки, ориентированные на системных архитекторов, администраторов, сервисных инженеров и других IT-специалистов, участвующих в планировании, проектировании и внедрении комплексных решений.

! Представленная информация основана на результатах исследований, а также экспертизе специалистов YADRO. Документ носит не предписывающий, а информационный характер, целью которого является информирование получателей документа о предмете произведенного исследования и о его результатах. При этом конкретные результаты и эффективность конечных решений зависят от множества факторов, которые могут различаться в зависимости от особенностей инфраструктуры и условий эксплуатации. Ни при каких обстоятельствах YADRO не несет ответственность за последствия применения получателем документа рекомендаций, инструкций, подходов и решений, указанных в документе.

Запрещается копировать, воспроизводить, изменять, публиковать, передавать, распространять, продавать информацию (часть информации), содержащуюся в документе, или создавать производные работы на основе содержания документа без предварительного письменного разрешения YADRO.

Любая информация или утверждения относительно возможностей, емкости, производительности или других характеристик продукции, указанной в документе, предоставляются исключительно на условиях «как есть» и приведена исключительно в целях описания произведенного исследования. YADRO оставляет за собой право вносить изменения/обновлять информация в документе без уведомления.

«YADRO» является зарегистрированным товарным знаком ООО «КНС ГРУПП». Другие названия продуктов и компаний, упомянутые здесь, могут быть товарными знаками или торговыми наименованиями их соответствующих владельцев.

Актуальные версии документации публикуются на информационном ресурсе YADRO по адресу service.yadro.com.

ОГЛАВЛЕНИЕ

1. ОБ ЭКСПЕРТАХ 4
2. ВВЕДЕНИЕ 5
3. НАСТРОЙКИ TATLIN.BACKUP 6
   - 3.1. Общие рекомендации по конфигурации системы TATLIN.BACKUP.M 6
   - 3.2. Создание файловых систем 7
   - 3.3. Создание файловых ресурсов NFS 8
   - 3.4. Создание файловых ресурсов CIFS/smb 8
   - 3.5. Создание точки монтирования NFS на UNIX-клиенте 9
4. НАСТРОЙКИ VEEAM BACKUP & REPLICATION 9
   - 4.1. Добавление хостов виртуализации 10
5. НАСТРОЙКА CIFS/SMB ДЛЯ VEEAM BACKUP & REPLICATION 11
   - 5.1. Настройка ресурса с общим доступом по протоколу SMB/CIFS в качестве целевого хранилища резервных копий 11
   - 5.2. Выполнение тестового резервного копирования 14
6. НАСТРОЙКА NFS ДЛЯ VEEAM BACKUP & REPLICATION 14
   - 6.1. Настройка NFS-папки как целевого хранилища резервных копий 14
7. ПОДГОТОВКА К РЕЗЕРВНОМУ КОПИРОВАНИЮ 14
   - 7.1. Рекомендуемые настройки заданий резервного копирования 14
   - 7.2. Планирование операций 15
   - 7.3. Общие рекомендации по конфигурации Veeam Backup & Replication 16
   - 7.4. для резервного копирования на хранилище с дедупликацией 16
   - 7.5. Добавление Linux-сервера в инфраструктуру резервного копирования 18
   - 7.6. Настройка репозитория резервных копий на NFS 20
   - 7.7. Выполнение тестового резервного копирования 21
   - 7.8. Выполнение восстановления 22
   - 7.9. Рекомендации по настройке сети Ethernet 23
8. НАСТРОЙКИ KORNFELD 23
   - 8.1. Настройка MC-LAG 23
   - 8.2. Предварительная настройка 24
   - 8.3. Настройка Bonding 25
   - 8.4. Настройка Jumbo Frames 25
9. НАСТРОЙКИ TATLIN.BACKUP 26
   - 9.1. Настройка Bonding из CLI 26
10. НАСТРОЙКИ ESXI 28
    - 10.1. Настройка Bonding 28
    - 10.2. Сетевые порты 29

ОБ ЭКСПЕРТАХ

Алексей Головин — специалист с 15-летним опытом работы в IT, включая опыт в таких компаниях, как Dell EMC и системных интеграторах. В 2022 году присоединился к команде YADRO в должности ведущего специалиста по интеграционным решениям. В YADRO Алексей поддерживает сложную инфраструктуру корпоративных клиентов. Занимается настройкой, оптимизацией и обслуживанием хранилищ данных и инфраструктуры резервного копирования. Специализируется на диагностике и устранении неисправностей систем YADRO, Dell EMC и других компаний-производителей.

ВВЕДЕНИЕ

Данный документ предназначен для ИТ-специалистов и администраторов, ответственных за внедрение и поддержку системы хранения данных TATLIN.BACKUP.M (далее — TATLIN.BACKUP.M, СХД). Документ содержит рекомендации по настройке и оптимизации TATLIN.BACKUP.M, а также по интеграции с системой резервного копирования и восстановления виртуальных машин Veeam Backup & Replication (далее — Veeam Backup & Replication, СРК) для достижения максимальной производительности, отказоустойчивости и безопасности данных.

Целевая аудитория включает технических специалистов, инженеров по безопасности данных и администраторов систем хранения, которым требуется обеспечить эффективную работу инфраструктуры резервного копирования с учетом современных требований к управлению данными и восстановлениям.

ВЕРСИИ ИСПОЛЬЗУЕМОГО ПО	
TATLIN.BACKUP.M	1.1, 1.2
Veeam Backup & Replication	12.1

НАСТРОЙКИ TATLIN.BACKUP

ТЕКУЩИЕ ЛИМИТЫ TATLIN.BACKUP.M	
Максимальный размер файла	16 ТБ
Максимальный размер файловой системы	693.3 ТБ / 630.6 ТиБ
Максимальное количество виртуальных файловых систем на ТВ-систему	64 виртуальных файловых системы / ресурса с общим доступом
Максимальное количество пользователей	59 000
Максимальное число файлов на систему	64 виртуальных файловых системы × 500 каталогов × 100 000 файлов в каталоге
Максимальное число файлов на один каталог	100 000
Максимальное число каталогов в VFS	500
Максимальное количество потоков на запись	400
Максимальное количество потоков на чтение	200

Общие рекомендации по конфигурации системы TATLIN.BACKUP.M

1. Максимальная скорость чтения/записи достигается при использовании двух и более дисковых модулей расширения.
   В минимальной конфигурации с одним дисковым модулем расширения скорость первого резервного копирования может быть ниже.
2. Для оптимальной работы T-RAID (для оптимального распределения дисков по группам аллокации) рекомендуется производить увеличение дисковой емкости целыми дисковыми модулями.
3. На TATLIN.BACKUP.M рекомендуется создать несколько виртуальных файловых систем, поскольку параллельная запись в несколько файловых систем позволяет достичь более высокой скорости. Рекомендуется создать 4–16 виртуальных файловых систем, каждая из которых должна обрабатывать по 4–16 потоков данных.
4. В целях повышения отказоустойчивости при передаче данных по Ethernet-соединениям рекомендуется использовать технологию агрегации каналов LACP.
5. Если к СХД подключаются более одного хоста или более чем из одной подсети, рекомендуется использовать две LACP-агрегации с портами из разных сетевых карт (`bond0:data0p0`, `data1p1` и `bond1:data0p1`, `data1p0`).
6. Если доступ к TATLIN.BACKUP.M осуществляется через один отказоустойчивый хост, рекомендуется использовать одну LACP-агрегацию (`bond0:data0p0`, `data0p1`, `data1p0`, `data1p1`).
7. На сетевых data-интерфейсах рек омендуется использовать jumbo-фреймы с MTU 9000 для эффективного использования каналов.
8. Рекомендации по настройке LACP в файловых системах:
   - Выбор метода балансировки (Transmit Hash Policy)
     Layer2+3 (MAC + IP) — рекомендуется при использовании нескольких IP-адресов на агрегированном интерфейсе. Обеспечивает равномерное распределение трафика.
     Layer3+4 (IP + TCP/UDP Port) — используется при динамическом распределении нагрузки, но не гарантирует равномерного распределения.
   - Настройка LACP для файловых систем:
     - **NFS**
       Layer2+3 с несколькими IP-адресами — предпочтительно.
       Layer3+4 применим с nconnect=<N> для увеличения числа соединений.
     - **CIFS**
       Layer2+3 — стабильное распределение трафика.
       Layer3+4 допустим при отсутствии дополнительных IP-адресов.
     - **T-Boost**
       Layer2+3 предпочтителен при работе с несколькими виртуальными файловыми системами.
9. Рекомендуется выбирать версию NFS в зависимости от поддерживаемой версии на хосте или в ПО СРК.
   При наличии поддержки NFSv4 предпочтительно использовать именно ее.

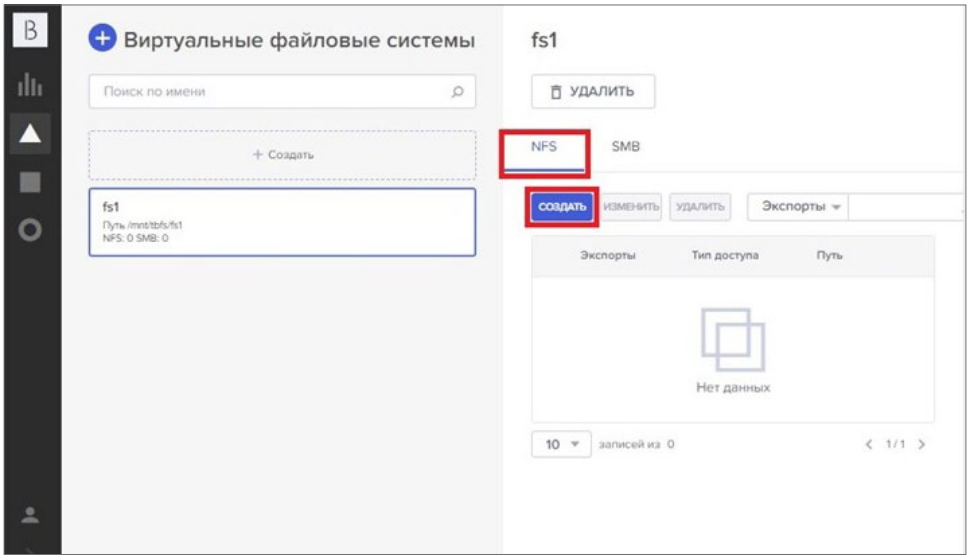
10. При монтировании по NFS рекомендуем использовать следующие опции:
    - Использовать mount-опцию `-o write=eager`
    - Не использовать `direct` при записи
    - Убедиться, что NFS примонтирован с `rsize/wsize` 1 Mb (1048576 байт)
11. Для достижения большей скорости обмена данными с TATLIN.BACKUP.M рекомендуется отдавать предпочтение I/O со следующими характеристиками:
12. Разделение по направлению передачи данных (read или write, не смешанный read/write).
    - Большой блок данных: 1–4 МиБ.
    - Последовательное выполнение операций.
    - Наличие нескольких I/O потоков на виртуальной файловой системе: 4–16 I/O потоков в каждую из 4–16 виртуальных файловых систем.
13. Оптимальная производительность TATLIN.BACKUP.M достигается при совершении операций 32 потока, равномерно распределенных по виртуальной файловой системе.
14. Для эффективного использования механизма дедупликации рекомендуется отключить механизм дедупликации на уровне CPK.

Создание файловых систем

1. Перейдите в **Хранилище**.
2. Создайте виртуальную файловую систему:
    - Нажмите **Создать** или значок в верхнем левом углу экрана.
    - Введите имя файловой системы. Например, **fs1**.
    - Нажмите **Создать**.
3. Убедитесь, что в **Хранилище** в списке файловых систем для созданной файловой системы отображается путь `/mnt/tbfs/fs1`. Если путь отображается, файловая система успешно создана и примонтирована.
4. Повторите шаги 2–3 для создания второй файловой системы, например, **fs2**.

Создание файловых ресурсов NFS

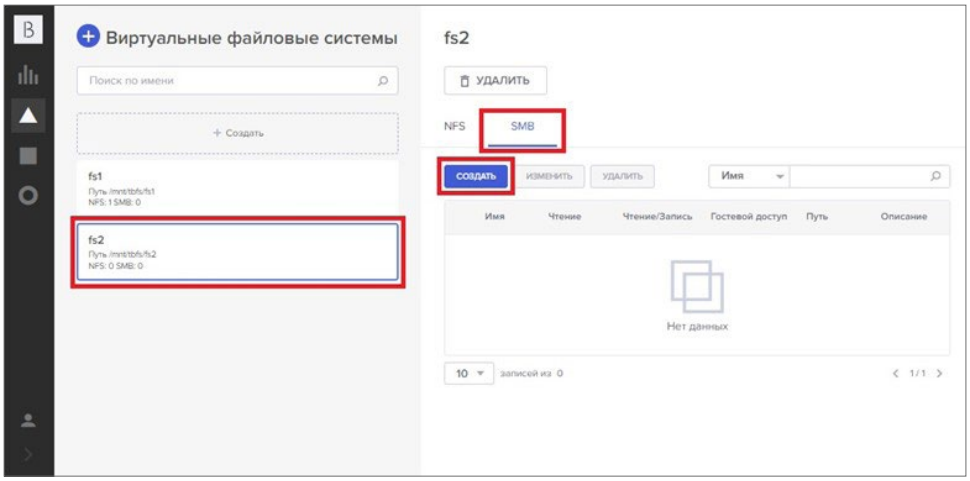
1. На вкладе **Хранилище** выбрать файловую систему **fs1**.
2. На вкладке **NFS** нажмите **Создать**.



3. Укажите необходимые значения:
   - В поле **IP-адрес** введите * для предоставления доступа по IP-адресам без ограничений.
   - В поле **Тип доступа** выберите **Чтение/Запись**.
4. Убедитесь, что созданный экспорт появился в списке экспортов NFS.

Создание файловых ресурсов CIFS/smb

1. В Хранилище выберите виртуальную файловую систему fs2.
2. На вкладке SMB нажмите Создать.



3. Укажите необходимые значения:
   - В поле **Имя** введите имя ресурса, например, **fs2guest**.
   - В поле **Гостевой доступ** выберите **Чтение/Запись**.
4. Убедитесь, что созданный экспорт появился в списке экспортов SMB.

Создание точки монтирования NFS на UNIX-клиенте

Чтобы настроить точку монтирования NFS на UNIX-клиенте для доступа к нужному хранилищу, выполните следующие шаги:

1. Создайте локальную директорию для монтирования.
2. С правами пользователя root создайте директорию, в которой будет смонтирован ресурс с общим доступом по протоколу NFS:

```
mkdir /mnt/tb
```

3. Смонтируйте удаленный NFS-ресурс в локальную директорию. Используйте команду mount с указанием нужных опций для используемой ОС.

Пример команды монтирования NFS-ресурса с TATLIN.BACKUP.M с настройками для оптимальной производительности:

```
mount -t nfs -o nolock,hard,intr,vers=3,tcp, rsize=32768,wsize=32768,bg
<TBHOSTNAME>:/data/<VFS> /mnt/tb
```

4. Проверьте монтирование:

```
ls -ltr /mnt/tb
```

НАСТРОЙКИ VEEAM BACKUP & REPLICATION

Перед выполнением задач защиты данных и восстановления после сбоев в Veeam Backup & Replication настройте инфраструктуру для резервного копирования. Архитектура инфраструктуры резервного копирования может различаться в зависимости от вашей виртуальной среды и стратегии резервного копирования.

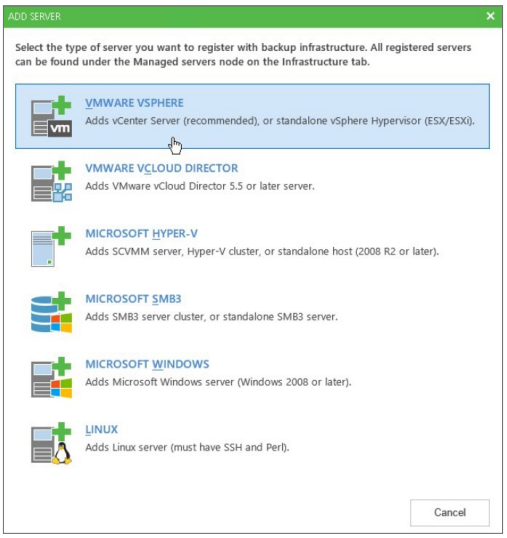
Типичная инфраструктура резервного копирования состоит из следующих компонентов:

- **Сервер резервного копирования Veeam** — сервер, на котором установлено программное обеспечение Veeam Backup & Replication.
- **Серверы виртуальной инфраструктуры** — хосты виртуализации, используемые в качестве источников и целевых серверов для резервного копирования, репликации и других задач.
- **Прокси-серверы для резервного копирования** — серверы, выполняющие роль «переносчиков данных». По умолчанию роль прокси-сервера назначается серверу резервного копирования Veeam или исходному хосту Hyper-V. Однако можно настроить выделенные прокси-серверы для резервного копирования. Подробную информацию можно найти в Руководстве пользователя Veeam Backup & Replication.
- **Репозитории** — хранилища для резервных копий, вспомогательных файлов реплик и копий виртуальных машин (далее — ВМ).

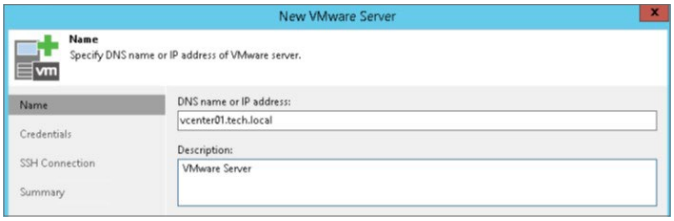
Добавление хостов виртуализации

Добавьте серверы VMware vSphere или Microsoft Hyper-V, чтобы использовать их в качестве источников и целевых расположений для резервного копирования, репликации и других операций.

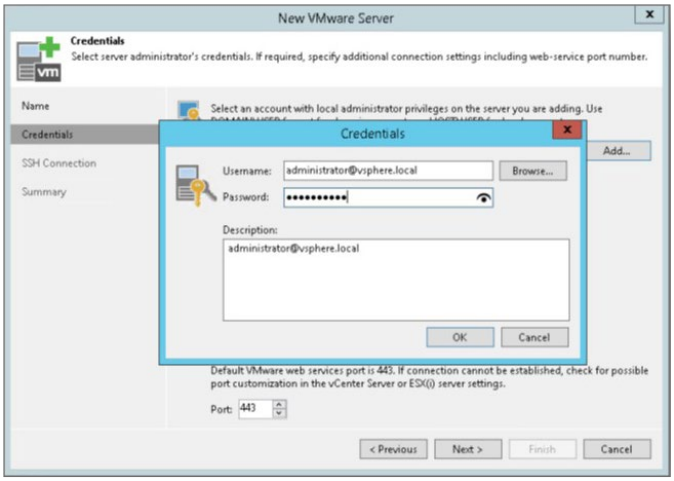
1. Выберите узел **Backup Infrastructure** — **Managed servers** в панели инвентаризации и нажмите **Add Server**.
2. Выберите **VMware vSphere** или **Microsoft Hyper-V**.



3. Укажите доменное имя или IP-адрес сервера, добавьте описание для справки.



4. Укажите учетные данные и параметры порта для подключения к серверу.



5. Просмотрите сводку конфигурации сервера и нажмите **Finish**.

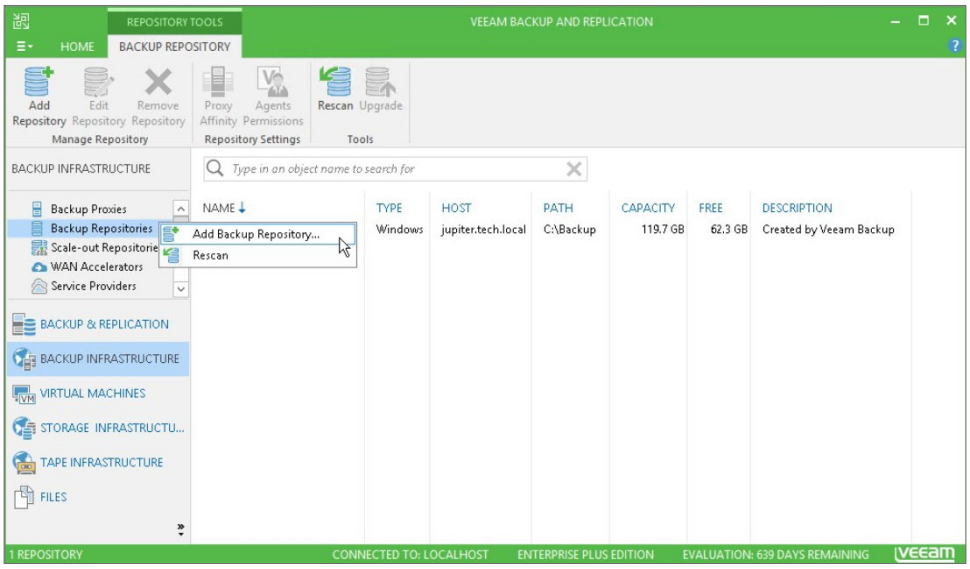
НАСТРОЙКА CIFS/SMB ДЛЯ VEEAM BACKUP & REPLICATION

Чтобы настроить ресурс с общим доступом по протоколу SMB/CIFS на TATLIN.BACKUP.M в качестве целевого хранилища, выполните тестовое резервное копирование и восстановите файл в Windows-среде.

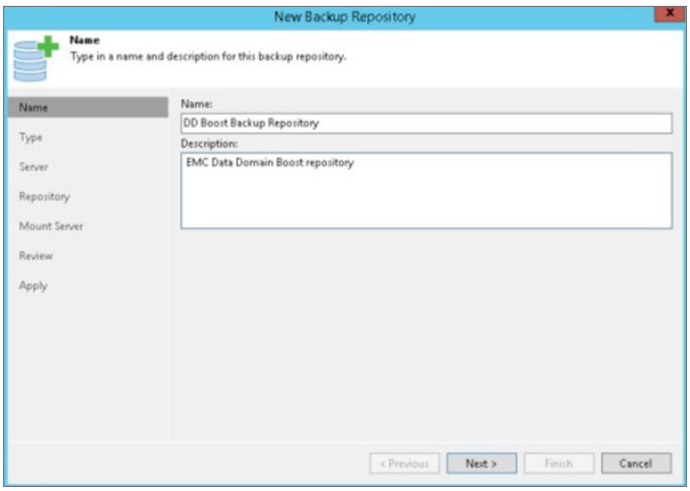
Настройка ресурса с общим доступом по протоколу SMB/CIFS в качестве целевого хранилища резервных копий

Ресурсы с общим доступом по протоколу SMB/CIFS на TATLIN.BACKUP.M могут использоваться для хранения резервных копий. SMB-хранилище упрощает процесс настройки, однако для Veeam Backup & Replication его пропускная способность ниже по сравнению с NFS-хранилищем. Протокол SMB/CIFS можно использовать в небольших средах (объем виртуальных машин до 3 ТБ) или там, где не допускается использование Linux-систем.

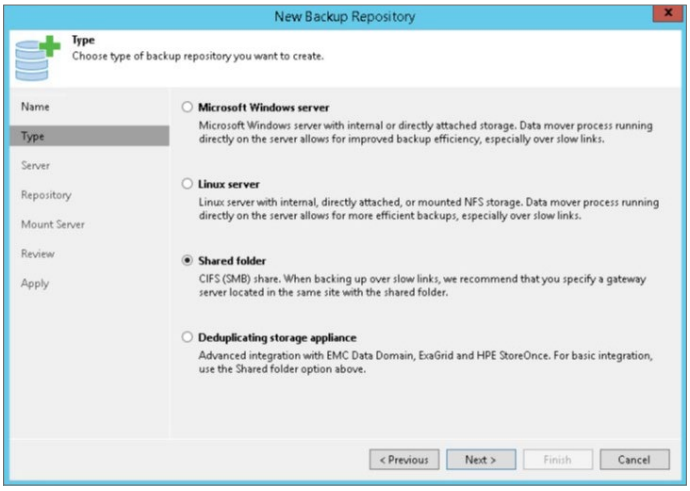
1. Перейдите в **Backup Infrastructure** – **Backup Repositories** – **Add Backup Repository.**



2. На вкладке **Name** укажите имя и описание для репозитория резервных копий.



3. На вкладке **Type** выберите **Shared folder**.

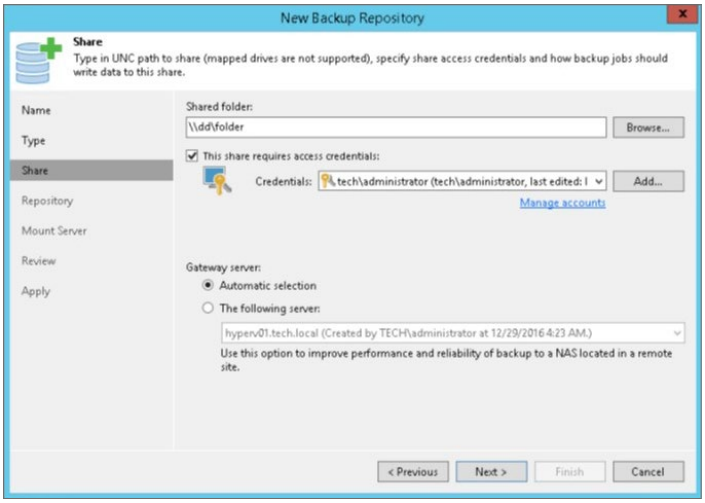


1. На вкладке **Share** укажите путь к общей папке на TATLIN.BACKUP.M.
   Установите флажок **This share requires access credentials**, укажите имя пользователя и пароль от учетной записи, имеющей доступ к общей папке.

> **!** Если у всех серверов есть права доступа к этой папке, учетные данные указывать не требуется.

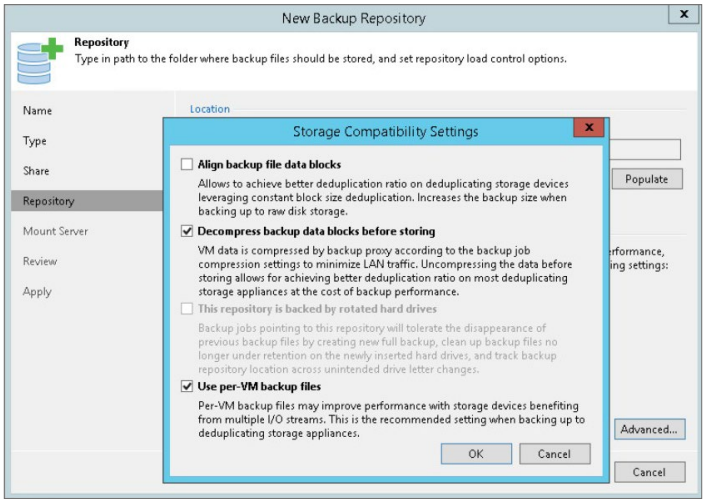
В блоке **Gateway server** задайте параметры для шлюза:

- Если соединение между исходным хранилищем и репозиторием резервных копий быстрое, выберите **Automatic selection**.
  В этом случае Veeam Backup & Replication автоматически выберет шлюзовый сервер.
- Если резервное копирование и репликация выполняются посредством WAN или при медленном соединении:
  1. Выберите **The following server**.
  2. Выберите из списка сервер **Microsoft Windows** на целевой площадке, который будет использоваться в качестве шлюза.
     Выбранный сервер должен иметь прямой доступ к общей папке и находиться как можно ближе к ней.
- В некоторых случаях автоматический выбор может вызвать проблемы, так как Veeam Backup & Replication может использовать разные шлюзовые серверы для разных сеансов задания. Например, при одном сеансе может использоваться 64-разрядный шлюзовый сервер для создания файла резервной копии, а при следующем — 32-разрядный, что приведет к ошибке при попытке открыть созданный файл резервной копии. Чтобы избежать этой ситуации, рекомендуется указать шлюзовый сервер.

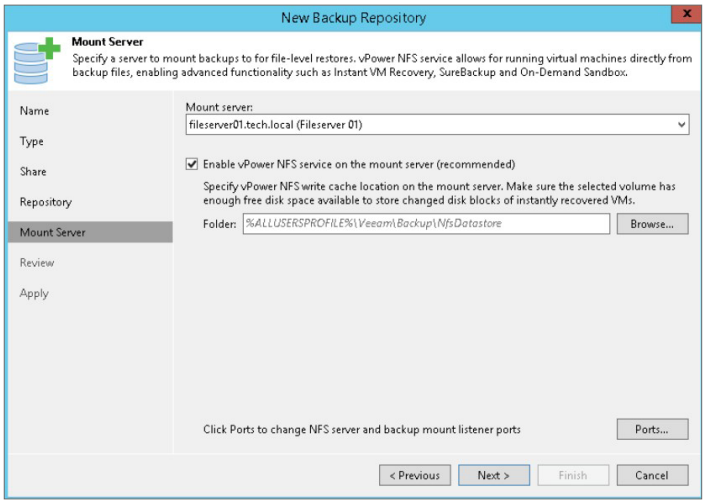


5. На вкладке **Repository** примените следующие настройки:
   - Снимите флажок **Align backup file data blocks**.
   - Установите флажок **Decompress backup data blocks before storing**.
   - Установите флажок **Use per-VM backup files**.

> **!** Если Veeam Backup & Replication был обновлен с предыдущих версий до версии 9.5, то эта опция будет отключена для совместимости с существующими репозиториями. Для создания цепочек резервных копий на ВМ можно изменить настройки репозитория и включить эту опцию.



6. На вкладке **Mount Server** укажите параметры для сервера монтирования, который будет использоваться для восстановления на уровне файлов и приложений:
   - В списке **Mount Server** выберите сервер, который будет использоваться в качестве сервера монтирования. С помощью сервера монтирования Veeam Backup & Replication будет монтировать диски ВМ из файла резервной копии в репозитории для ускоренного восстановления, без загрузки данных по сети.
   - Установите флажок **Enable vPower NFS server on the mount server**, чтобы сделать репозиторий доступным для службы Veeam vPower NFS. Veeam Backup & Replication активирует службу vPower NFS на выбранном сервере монтирования.
   - В поле **Folder** укажите папку, которая будет использоваться в качестве корневой.



7. Следуйте дальнейшим шагам мастера установки, не изменяя настройки по умолчанию. На вкладке **Summary** нажмите **Finish**, чтобы завершить настройку репозитория резервных копий.

Свяжитесь с нами:
support@yadro.com
www.yadro.com
Москва, ул. Рочдельская, 15, стр.13
+7 800 777-06-11

Выполнение тестового резервного копирования

В Veeam Backup & Replication процесс резервного копирования управляется заданиями. Для резервного копирования ВМ необходимо настроить задание на резервное копирование. Задание определяет, как, где и когда следует выполнять резервное копирование данных ВМ. Одно задание может использоваться для обработки одной или нескольких ВМ.

Veeam Backup & Replication выполняет резервное копирование образа ВМ целиком, копируя данные ВМ на блочном уровне, извлекая их из исходного хранилища и записывая их в репозиторий резервных копий в проприетарном формате Veeam Backup & Replication. Резервные копии на уровне образа подходят для всех типов сценариев восстановления данных, таких как полное восстановление ВМ, восстановление файлов и папок гостевой ОС ВМ, а также восстановление файлов ВМ и виртуальных дисков ВМ (только для ВМ на VMware) из файла резервной копии.

Veeam Backup & Replication поддерживает как полные, так и инкрементные резервные копии. При первом запуске задания Veeam Backup & Replication создает полную резервную копию ВМ (VBK-файл).

Все последующие циклы задания создают инкрементные резервные копии, тип которых зависит от выбранного метода:

- **VIB** — если используется метод «постоянного прямого инкрементного» или «прямого инкрементного» резервного копирования.
- **VRB** — если используется метод «обратного инкрементного» резервного копирования.

Количество хранимых инкрементных резервных копий зависит от настроек политики хранения.

НАСТРОЙКА NFS ДЛЯ VEEAM BACKUP & REPLICATION

Настройка NFS-папки как целевого хранилища резервных копий

Резервные копии можно сохранять в NFS-экспорт, смонтированный с системы TATLIN.BACKUP.M на промежуточную Linux-систему.

Для поддержки ресурса с общим доступом по протоколу NFS в Veeam Backup & Replication требуется промежуточная Linux-система, поскольку:

- служба vPower NFS в Veeam Backup & Replication не поддерживает прямое подключение к ресурсам с общим доступом по протоколу NFS;
- системы Microsoft Windows не оптимизированы для работы с NFS.

Такая конфигурация рекомендуется как для сред VMware vSphere, так и для Microsoft Hyper-V.

ПОДГОТОВКА К РЕЗЕРВНОМУ КОПИРОВАНИЮ

> **!** Раздел описывает основные шаги для создания задания на резервное копирование. Более подробная информация представлена в разделе «Создание заданий на резервное копирование» в документе «Руководство пользователя Veeam Backup & Replication».

Рекомендуемые настройки заданий резервного копирования

Для обеспечения оптимальной работы системы TATLIN.BACKUP в среде резервного копирования с использованием Veeam Backup & Replication следуйте приведенным ниже рекомендациям и передовым практикам.

Размер блока при записи:

- Для NFS: используйте размер блока записи 1 МБ.
- Для SMB: предпочтительно использовать 4 МБ.

Оптимизация данных:

- Избегайте записи множества мелких файлов. Вместо этого объедините их в один крупный архив для более эффективной обработки и хранения.

Первая копия:

- Постарайтесь для первой резервной копии выбрать источники с максимальным количеством уникальных блоков данных, чтобы оптимизировать дедупликацию.

Группировка данных для дедупликации:

- В настройках задания (Плане защиты) объединяйте однотипные виды данных. Либо настраивайте задания для разных типов данных так, чтобы их создание не происходило одновременно. Это поможет улучшить дедупликацию.

Шифрование и защита данных:

- Отключите шифрование на уровне резервной копии (СРК), поскольку это может затруднить дедупликацию.
- Не используйте защиту паролем на уровне резервной копии — установите защиту на уровне хранилища для максимального эффекта от дедупликации.

Сжатие данных:

- Установите уровень сжатия данных в резервных копиях на режим «Нет» или «Обычный» для оптимальной производительности хранения.

Глубина хранения и частота резервных копий:

- Чем чаще создаются резервные копии и выше глубина хранения, тем эффективнее будет использование TATLIN.BACKUP.

Разделение критичных данных:

- Разделяйте различные типы критичных данных по отдельным устройствам хранения, а также создавайте реплики копий на другие типы хранилищ для дополнительной безопасности.

Методы резервного копирования:

- Обратите внимание, что TATLIN.BACKUP не поддерживает метод резервного копирования с обратной инкрементной копией.

Профиль набора данных

- TATLIN.BACKUP эффективно поддерживает до 100 миллионов файлов. При превышении этого лимита производительность системы может значительно снизиться. При планировании системы, на которой будут размещаться как резервные копии, так и архивы, учитывайте это ограничение.

Планирование операций

Планирование резервного копирования и репликации:

- Настройте выполнение операций резервного копирования и репликации до начала рабочего дня, чтобы избежать нарушений доступа пользователей к системе TATLIN.BACKUP.

Политики резервного копирования:

- Учитывайте фоновую нагрузку от операций при настройке политик резервного копирования и планировании других задач.

Регулярная очистка данных:

- Настройте регулярную очистку данных на ежедневной, еженедельной или ежемесячной основе, особенно если объем данных составляет миллионы файлов. Это позволит поддерживать оптимальную производительность хранилища.

Общие рекомендации по конфигурации Veeam Backup & Replication для резервного копирования на хранилище с дедупликацией

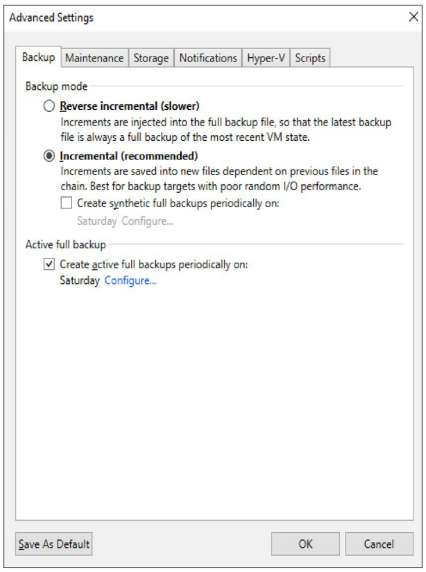
Настройки задания:

- Согласно статье **Veeam KB1 745**, все рекомендации от производителя и конкретные советы производителя имеют приоритет над приведенными ниже рекомендациями.

Настройки задания на резервное копирование:

- Чтобы задать дополнительные настройки, перейдите в **Storage** – **Advanced**.

Вкладка Backup (Резервное копирование):



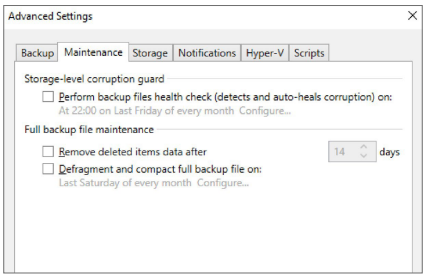
- Обычно устройства дедупликации показывают низкую производительность при чтении данных.
  Чтобы максимизировать производительность, задания резервного копирования должны быть настроены на запись без операций чтения.
  Настройте задание на резервное копирование с использованием метода **Incremental (Forward)** с еженедельными **Active Full**.

> ! Некоторые устройства для дедупликации, интегрированные с Veeam Backup & Replication, могут выполнять синтетическое полное копирование **Synthetic Full**.

Активное полное копирование: включено и настроено на еженедельное выполнение
Еженедельные точки полного восстановления позволяют сократить количество точек восстановления, необходимых для чтения во время восстановления.

Чтобы настроить задание на активное полное копирование:
1. Включите опцию **Incremental**.
2. Установите флажок **Create active full backups periodically on:**.
3. Нажмите **Configure** и настройте еженедельное выполнение резервного копирования.

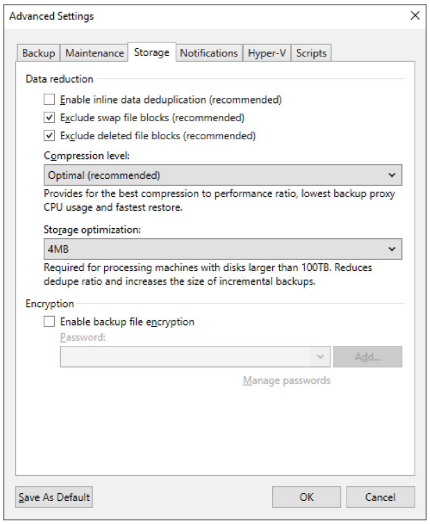
Вкладка Maintenance (Обслуживание)



- **Проверка состояния файлов резервных копий: отключена**
  Включение этой функции на хранилищах с дедупликацией возможно, но она требует большого количества операций чтения и может занять значительное время. С большими файлами на хранилище с дедупликацией эта функция может привести к тому, что задание будет выполняться днями, мешая созданию новых точек восстановления.
  Чтобы отключить проверку состояния файлов резервных копий, снимите флажок **Perform backup files health check (detects and auto-heals corruption) on:**

- **Дефрагментация и компактная упаковка полного файла резервной копии: отключена**
  Включение этой опции не требуется, если создаются активные полные копии.
  Чтобы отключить дефрагментацию и компактную упаковку полного файла резервной копии, снимите флажок **Defragment and compact full backup file on:**

Вкладка Storage (Хранилище)



- **Встроенная дедупликация данных: отключена.**
  Отключение дедупликации в Veeam Backup & Replication делает точки восстановления больше, но позволяет дедупликации на уровне хранилища работать эффективнее.

> **!** Хранилища, использующие недедупликационные зоны для хранения файлов, могут извлечь пользу из включения дедупликации Veeam Backup & Replication, что позволит удерживать больше точек восстановления в зоне быстрого доступа перед обработкой системой дедупликации хранилища.

Чтобы отключить встроенную дедупликацию данных, снимите флажок **Enable inline data deduplication (recomended)**.

- **Уровень сжатия: Optimal или Dedupe-friendly**
  Рекомендуется включить функцию репозитория, которая будет распаковывать все точки восстановления перед их записью. Таким образом, уровень сжатия на уровне задания влияет только на сжатие данных при передаче по сети.

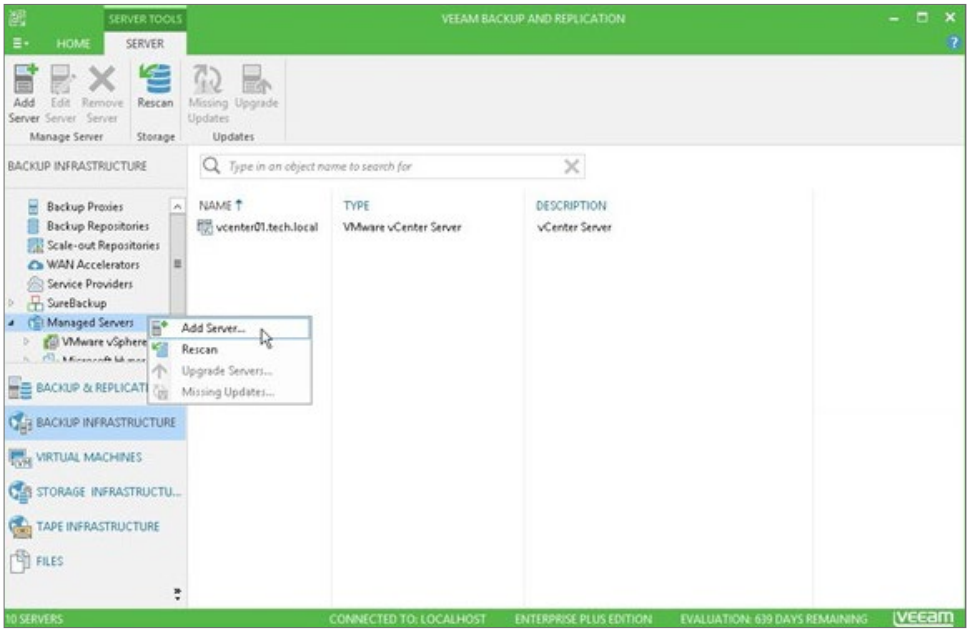
Полное отключение сжатия на уровне задания не рекомендуется, так как это значительно увеличит объем данных, передаваемых по сети. Чтобы снизить нагрузку на сеть, выберите в блоке **Compression level** уровень **Optimal** или **Dedupe-friendly** из выпадающего списка.

- **Оптимизация хранилища (размер блока): 4 МБ**
  Этот размер блока улучшает производительность при хранении резервных копий на хранилищах с дедупликацией, уменьшая размер внутренней таблицы метаданных резервной копии.
  Выберите в блоке **Storage optimization** размер блока 4 МБ.

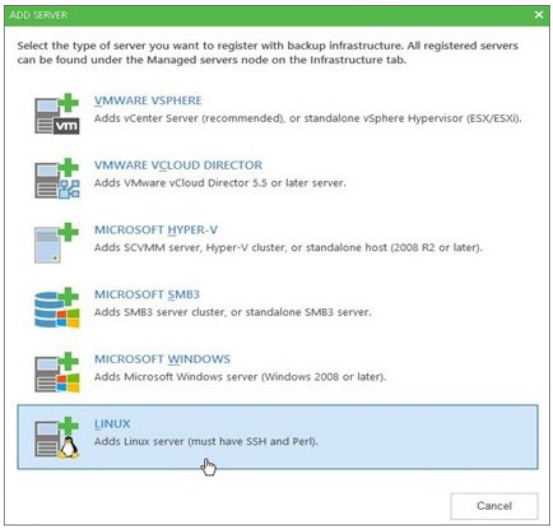
- **Шифрование: Отключено**
  Шифрование данных негативно влияет на коэффициент дедупликации при использовании хранилищ с дедупликацией, так как Veeam Backup & Replication использует разные ключи шифрования для каждой сессии задания. В результате шифрованные блоки данных, отправляемые на хранилище, выглядят разными, даже если содержат одинаковые данные. Для достижения высокого коэффициента дедупликации рекомендуется отключить шифрование. Если требуется использовать шифрование, включите функцию шифрования непосредственно на хранилище с дедупликацией.
  Чтобы отключить шифрование, снимите флажок **Enable backup file** encryption в блоке **Encryption**.

Добавление Linux-сервера в инфраструктуру резервного копирования

1. Перейдите в **Backup Infrastructure** — **Managed servers** — **Add Server**

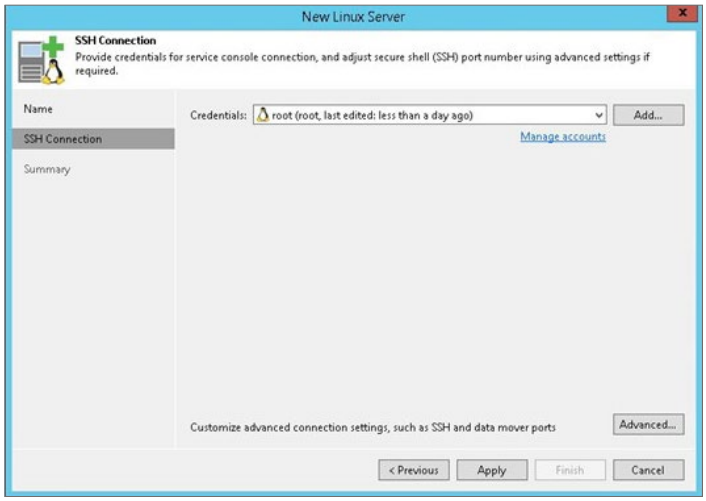


2. Нажмите **Linux**.



3. На вкладке **Name** укажите доменное имя или IP-адрес промежуточного Linux-сервера и добавьте описание для справки.

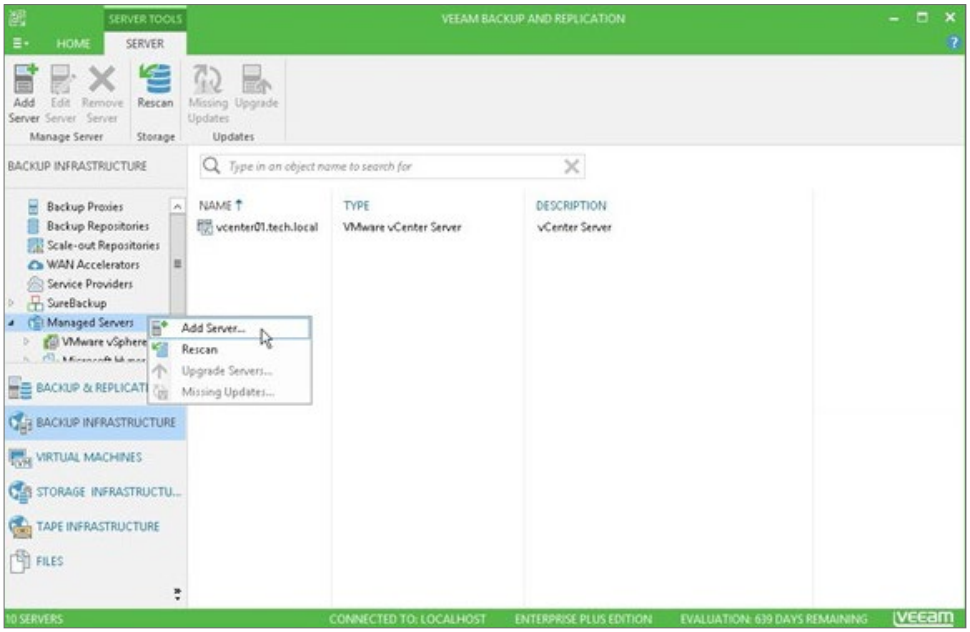




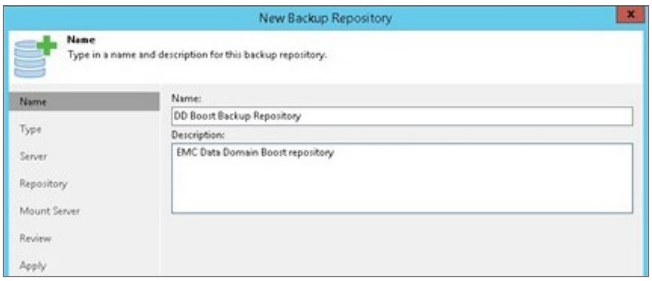
4. Следуйте следующим шагам мастера установки, не изменяя настройки по умолчанию. На вкладке **Summary** нажмите **Finish**, чтобы завершить настройку сервера.

Настройка репозитория резервных копий на NFS

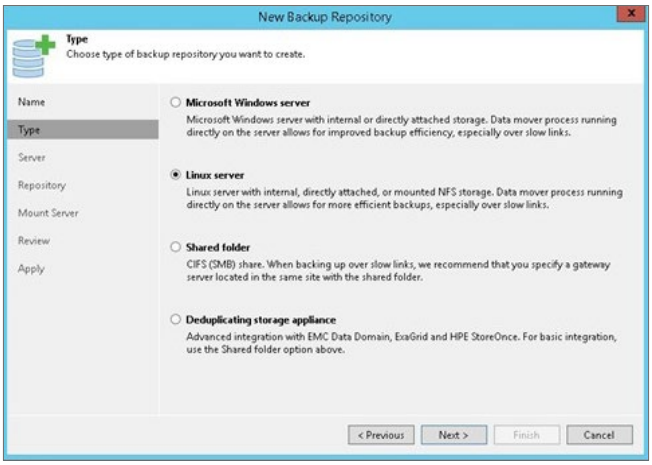
1. Перейдите в **Backup Infrastructure** – **Backup Repositories** – **Add Backup Repository**.



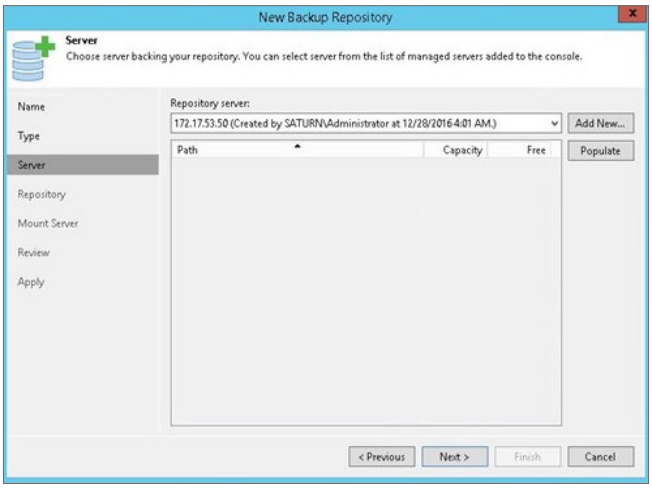
2. На вкладке **Name** укажите имя и описание для репозитория резервных копий.



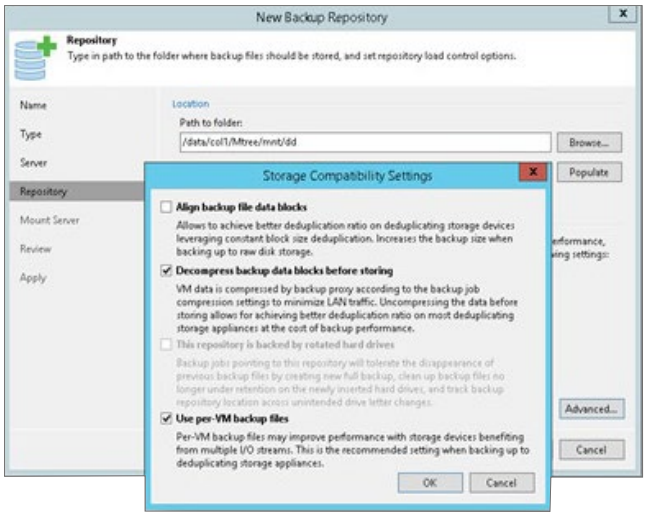
3. На вкладке **Type** выберите **Linux server**.



4. На вкладке **Server** выберите Linux-сервер, где смонтирован NFS-экспорт.



5. На вкладке **Repository** укажите путь к NFS-экспорту на виртуальной файловой системе TATLIN.BACKUP.M.
6. Нажмите **Advanced** и установите флажки **Decompress backup data blocks before storing** и **Use per-VM backup**.
   Если Veeam Backup & Replication обновлен до версии 9.5 с предыдущих версий, опция **Use per-VM backup files** будет выключена для обеспечения совместимости с существующими репозиториями. Для создания цепочек резервных копий по ВМ измените настройки репозитория и включите эту опцию.



7. Следуйте следующим шагам мастера установки, не изменяя настройки по умолчанию. На вкладке **Summary** нажмите **Finish**, чтобы завершить настройку репозитория резервных копий.

Выполнение тестового резервного копирования

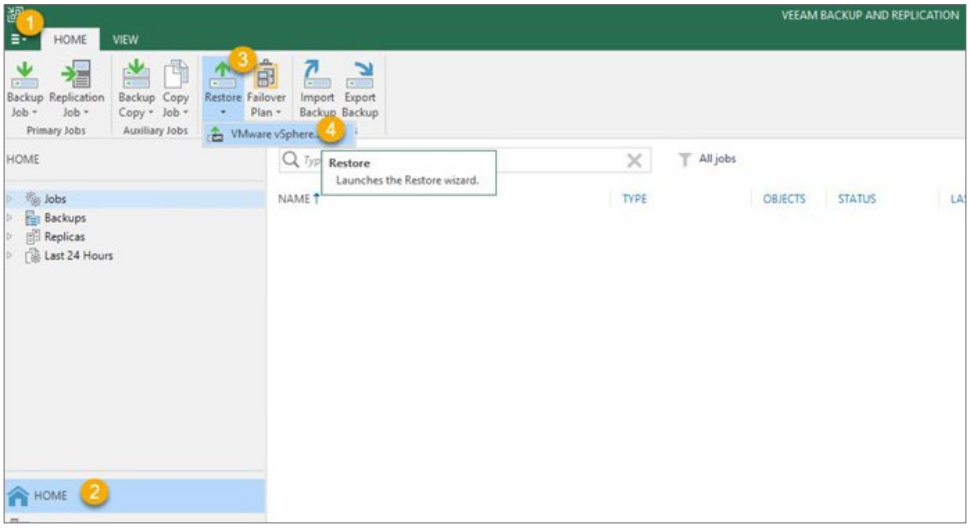
Процедура резервного копирования на NFS аналогична процедуре для CIFS/SMB. Выполните инструкции из раздела **Выполнение тестового резервного копирования** (стр. 14).

Выполнение восстановления

Вы можете восстановить виртуальные машины (VM), файлы и диски виртуальных машин, элементы приложений и отдельные файлы гостевой операционной системы до последнего состояния или до любой доступной точки восстановления. Восстановление может выполняться двумя методами:

Восстановление из резервной копии:

1. Войдите в консоль Veeam Backup and Replication.
2. Перейдите во вкладку **HOME**.
3. Нажмите **Restore**.
4. Выберите **VMware vSphere**.
5. Выберите **Restore from backup**.



6. Выберите тип восстановления. Доступны следующие варианты:
   - Полное восстановление ВМ (**Entire VM restore**) — восстанавливает всю ВМ или ее отдельные компоненты (виртуальные диски).
   - Мгновенное восстановление ВМ (**Instant VM recovery**).
7. Нажмите **Add** и добавьте нужные ВМ для восстановления:
   - Выберите **From infrastructure**, если необходимо восстановить из виртуальной инфраструктуры или vCenter.
   - Выберите **From backup**, если резервная копия хранится локально или на устройстве TATLIN.BACKUP.M.
8. На вкладке **Restore Mode** выберите режим восстановления. Укажите, следует ли восстанавливать ВМ в исходное расположение или в новое с измененными параметрами.
9. Выполните сканирование резервной копии на наличие вредоносных программ.
10. На вкладке **Reason** укажите причину восстановления и нажмите **Next**.
11. При необходимости сохраните конфигурацию восстановления для будущего использования.
12. Нажмите **Finish**.

Процесс восстановления займет несколько минут, после чего ВМ будут полностью восстановлены.

Рекомендации по настройке сети Ethernet

Можно выделить следующие рекомендации по настройке сетевых интерфейсов:

- Объединение интерфейсов LACP на всех элементах схемы СРК.
- Установите значение MTU 9000 при сетевом взаимодействии с TATLIN.BACKUP.M.

Ниже представлены примеры настроек на сетевых коммутаторах KORNFELD, TATLIN.BACKUP.M и сервере виртуализации.

НАСТРОЙКИ KORNFELD

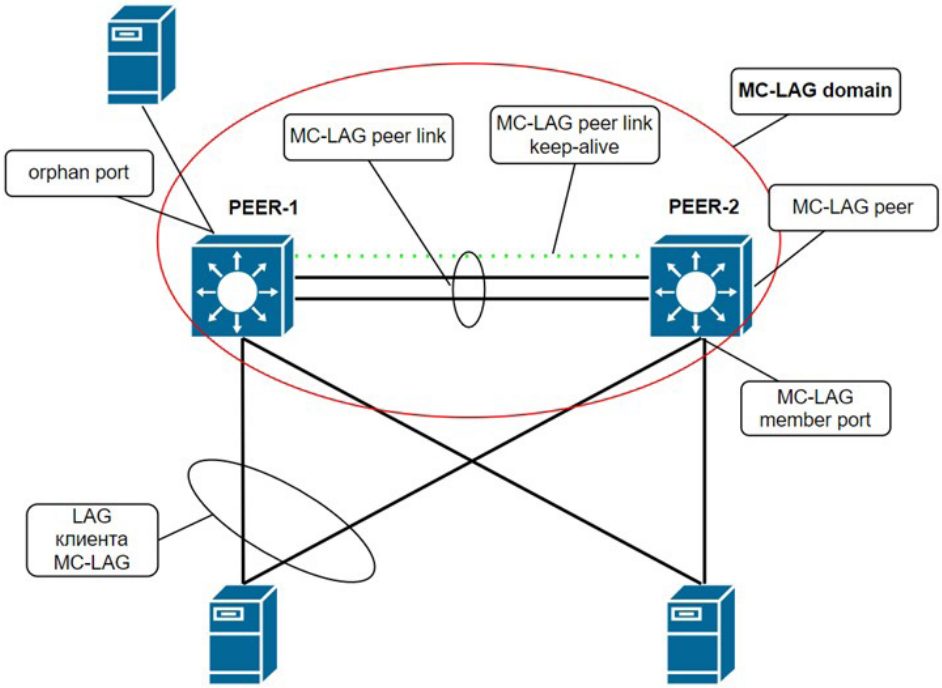
Настройка MC-LAG

MC-LAG — технология резервирования уровня узла, которая используется совместно с резервированием уровня канала, предоставленного LAG. Технология позволяет двум узлам, состоящим в домене MC-LAG, совместно использовать общую конечную точку LACP-агрегации. При этом коммутаторы домена остаются внешне совместимыми со стандартом LACP (**IEEE 802.1 AX-2008**).

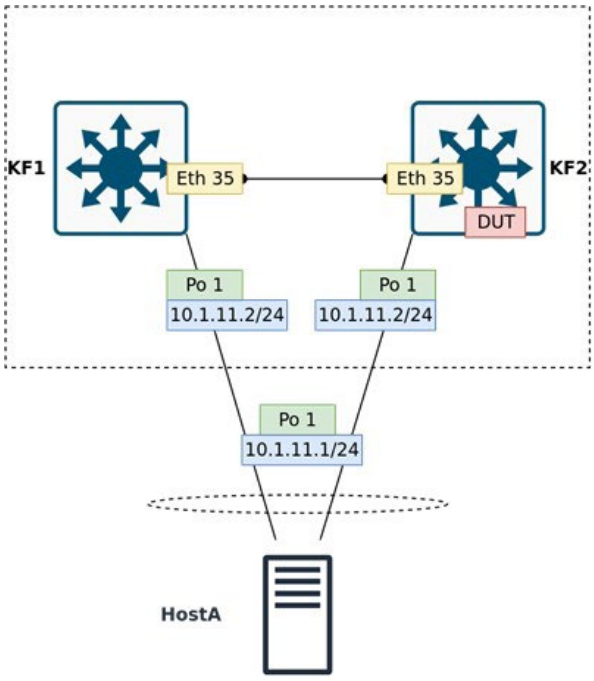
Клиенты MC-LAG физически подключаются к разным узлам, но к одной логической инфраструктуре с возможностью 100% резервирования. Для синхронизации и согласования процессов резервирования узлы в MC-LAG домене взаимодействуют между собой посредством протокола ICCP (**RFC 7275**).

Технология MC-LAG обеспечивает резервирование через соединения между двумя коммутаторами и отсутствие петель коммутации при работе сети на уровне L2 без использования протокола STP.

Использование MC-LAG позволяет нижестоящему клиентскому устройству, такому как коммутатор или сервер, сформировать агрегированный канал, будучи подключенным одновременно к двум коммутаторам. Нижестоящее (клиентское) устройство должно поддерживать агрегацию каналов с поддержкой протокола LACP, описанном в стандарте (IEEE 802.1 AX-2008).



Пример настройки MC-LAG для 2-х коммутаторов KORNFELD. Подробные инструкции см. на сайте производителя.



Предварительная настройка

1. На коммутаторе Kornfeld KF1 настройте MC-LAG.

```
KF1# configure terminal
KF1(config)# mclag domain 1
KF1(config-mclag-domain-1)#source-ip 10.10.10.1
KF1(config-mclag-domain-1)#peer-ip 10.10.10.2
KF1(config-mclag-domain-1)#no shutdown
KF1(config-mclag-domain-1)#exit
KF1(config)# interface Ethernet27 KF1(conf-if-Ethernet35)# ip address 10.10.10.1/24
```

2. На коммутаторе Kornfeld KF2 настройте MC-LAG.

```
configure terminal mclag domain 1 source-ip 10.10.10.2 peer-ip
10.10.10.1 no shutdown exit interface Ethernet27 ip address 10.10.10.2/24 exit
```

3. На клиентском устройстве HostA создайте L3-интерфейс PortChannel.

```
interface PortChannel 1 ip address 10.1.11.1/24 exit interface Ethernet 20 channel-group 1
exit interface Ethernet 21
channel-group 1
```

4. На коммутаторе Kornfeld KF1 создайте L3-интерфейс PortChannel и добавьте его в существующий домен MC-LAG.

```
KF1(config)# interface PortChannel 1
KF1(conf-if-po1)# ip address 10.1.11.2/24
KF1(conf-if-po1)# mclag 1
```

5. На коммутаторе Kornfeld KF2 создайте L3-интерфейс PortChannel и добавьте его в существующий домен MC-LAG.

```
interface PortChannel 1 ip address 10.1.11.2/24 mclag 1 exit
```

6. На коммутаторе Kornfeld KF1 добавьте в состав PortChannel интерфейс Ethernet, который подключен к клиентскому оборудованию HostA.

```
KF1# configure terminal
KF1(config)# interface Ethernet 20
KF1(conf-if-Ethernet20)# channel-group 1
KF1(conf-if-Ethernet20)# end
```

7. На коммутаторе Kornfeld KF2 добавьте в состав PortChannel интерфейс Ethernet, который подключен к клиентскому оборудованию HostA.

```
configure terminal
interface Ethernet 20
channel-group 1 end
```

Настройка Bonding

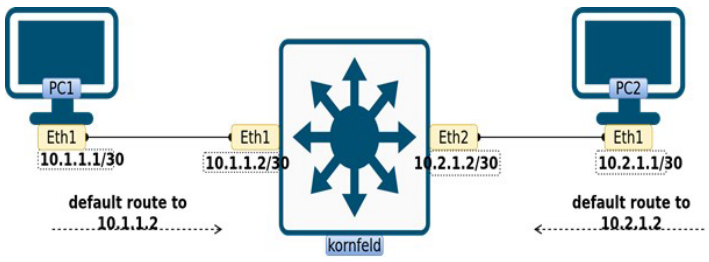
Проверим состояние LAG. Статус интерфейсов должен быть P, статус PortChannel — U.

```
kornfeld# show PortChannel summary Flags (oper-status): D - Down, U - Up (portchannel), P - Up in portchannel (members)
Flags (protocol): A - Active, P - Passive
-----------------------------------------------------------------------------------------------------------------
Group                                PortChannel              Protocol             Member Ports
-----------------------------------------------------------------------------------------------------------------
1                                    PortChannel1 (U)         LACP (A)             Ethernet33(P)
                                                                                   Ethernet34(P)
```

Настройка Jumbo Frames

При сетевом взаимодействии с TATLIN.BACKUP рекомендуемый параметр MTU = 9000.

Пример настройки:



1. Настройте IP-адрес, MTU и маршрут по умолчанию на PC1 (ubuntu).

```
[root@PC1 ~]$ ip addr add 10.1.1.1/30 dev eth1
[root@PC1 ~]$ ip link set dev eth1 mtu 9300
[root@PC1 ~]$ ip route add 10.0.0.0/14 via 10.1.1.2
```

2. Настройте IP-адрес, MTU и маршрут по умолчанию на PC2 (ubuntu).

```
[root@PC2 ~]$ ip addr add 10.2.1.1/30 dev eth1
[root@PC2 ~]$ ip route add 10.0.0.0/14 via 10.2.1.2
[root@PC2 ~]$ ip link set dev eth1 mtu 9300
```

3. Настройте IP-адреса на коммутаторе.

```
kornfeld-EC2# configure terminal kornfeld-EC2(config)# interface Ethernet 39
kornfeld-EC2(conf-if-Ethernet39)# ip address 10.1.1.2/30 kornfeld-EC2(conf-if-Ethernet39)#
exit kornfeld-EC2(config)# interface Ethernet 40 kornfeld-EC2(conf-if-Ethernet40)# ip address
10.2.1.2/30 kornfeld-EC2(conf-if-Ethernet40)# end
```

4. Проверьте, что между PC1 и PC2 есть IP-связность.

```
[root@PC1 ~]$ ping 10.2.1.1 -c 1 PING 10.2.1.1 (10.2.1.1) 56(84) bytes of data.
64 bytes from 10.2.1.1: icmp_seq=1 ttl=63 time=0.779 ms
--- 10.2.1.1 ping statistics --- 1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.779/0.779/0.779/0.000 ms
```

НАСТРОЙКИ TATLIN.BACKUP

Настройка Bonding из CLI

Создайте агрегированный интерфейс LACP:

```
tbcli network bond create lacp
```

Параметры команды:
--dhcp (string): Включение поддержки DHCP-клиента. Принимаемые значения: yes, no.
--hash-policy (string): Политика передачи хэша. Обязательный параметр. Возможные значения:

```
layer2
layer3+4
layer2+3
encap2+3
encap3+4
```

--ifaces (strings): Список подчиненных интерфейсов для указанного агрегированного интерфейса. Интерфейсы указываются через запятую.

```
Пример: --ifaces='eth0,eth1'
```

--ip (strings): IPv4-адреса интерфейса. Чтобы сбросить адрес, используйте пустое значение «».

```
Примеры: --ip='192.168.56.100/24' или --ip='192.168.40.122/24'
```

--ip-gw (string): Адрес шлюза по умолчанию. Чтобы сбросить адрес, используйте пустое значение «».

```
Пример: --ip-gw='192.168.56.1'
```

--json (bool): Вывод в формате JSON.
--mii-interval (uint32): Частота мониторинга состояния связи MII в миллисекундах. Определяет, как часто проверяется состояние связи для каждого слейва. Значение 0 отключает мониторинг.
--mtu (uint32): Максимальный размер пакета (MTU) в байтах.
--state (string): Включение/выключение интерфейса. Допустимые значения:

```
up — для включения
down — для отключения
```

--timeout, -t (duration): Тайм-аут для выполнения операции.

```
Примеры: 30s, 15m, 1h
```

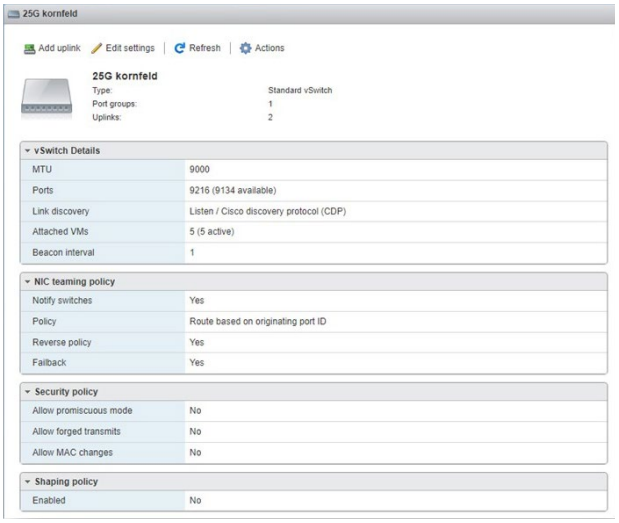
--transmit-rate (string): Частота, с которой партнер по связи передает пакеты LACP. Обязательный параметр. Возможные значения:

```
fast
slow
```

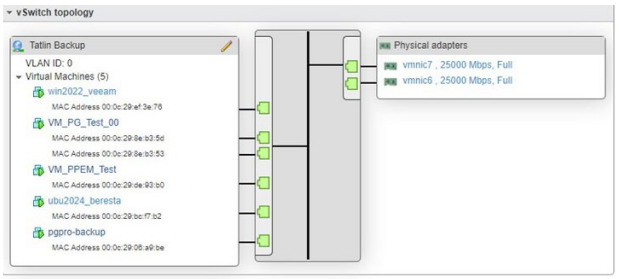
НАСТРОЙКИ ESXI

Настройка Bonding

Агрегация интерфейсов и MTU задаются на уровне Virtual switches:



Пример объединения двух физических Ethernet-интерфейсов 25 Гбит/с:



Сетевые порты

Veeam Backup & Replication автоматически создает правила брандмауэра для необходимых портов на компонентах инфраструктуры резервного копирования. Эти правила позволяют наладить связь между компонентами.

Автоматические правила брандмауэра для TCP-порта 1 1 1:

From	To	Protocol	Port	Notes
Backup server or gateway server	Dell Data Domain	TCP	111	Port used to assign a random port for the mountd service used by NFS and DDBOOST. Mountd service port can be statically assigned.

Автоматические правила брандмауэра для TCP-портов 2049 и 2052:

From	To	Protocol	Port	Notes
		TCP	2049	Main port used by NFS. Can be modified using the 'nfs set server-port' command. Command requires SE mode.
		TCP	2052	Main port used by NFS MOUNTD. Can be modified using the 'nfs set mountd-port' command in SE mode.