

IBM Spectrum Protect
версия 8.1.10

Руководство по решению на лентах



Примечание:

Прежде чем использовать эту информацию и описываемый в ней продукт, прочтите информацию в разделе [“Замечания” на стр. 235](#).

Замечания к изданию

Это издание относится к версии 8, выпуску 1, модификации 10 IBM Spectrum Protect (номера продукта 5725-W98, 5725-W99, 5725-X15) и ко всем его последующим выпускам и модификациям, пока в новых изданиях не будет указано иное.

© Copyright International Business Machines Corporation 1993, 2020.

Содержание

Об этой публикации.....	vii
Для кого предназначено это руководство.....	vii
Публикации	vii
Что нового.....	ix
Часть 1. Планирование.....	1
Требования к планированию лент.....	2
Требования к системе для решения на основе ленты.....	3
Требования к аппаратным средствам.....	3
Требования к программному обеспечению.....	7
Рабочие листы планирования.....	8
Планирование дисковой системы хранения.....	14
Планирование массивов хранения.....	15
Планирование ленточной системы хранения.....	16
Поддерживаемые ленточные устройства и библиотеки.....	17
Поддерживаемые конфигурации ленточных устройств.....	18
Перемещение данных между устройствами хранения.....	18
Совместное использование библиотек.....	19
перемещение данных в режиме без сети (LAN-free data movement).....	20
Смешанные типы устройств в библиотеке.....	21
Определения, необходимые для ленточных устройств хранения.....	23
Планирование иерархии пулов хранения.....	23
Хранение данных вне площадки.....	26
Планирование защиты.....	27
Планирование ролей администратора.....	27
Планирование защищенной связи.....	28
Планирование хранения зашифрованных данных.....	29
Планирование доступа через брандмауэр.....	29
Часть 2. Реализация.....	33
Настройка системы.....	34
Конфигурирование оборудования систем хранения.....	34
Установка операционной системы сервера.....	35
Установка в системах AIX.....	35
Установка в системах Linux.....	37
Установка в системах Windows.....	41
Конфигурирование ввода-вывода с несколькими путями.....	42
Системы AIX.....	42
Системы Linux.....	43
Системы Windows.....	45
Создание ID пользователя для сервера.....	45
Подготовка файловых систем для сервера.....	46
Системы AIX.....	46
Системы Linux.....	48
Системы Windows.....	49
Установка сервера и компонента Центр операций.....	49
Установка в системах AIX и Linux.....	49
Установка обязательных файлов RPM для графического мастера.....	50
Установка в системах Windows.....	51

Конфигурирование сервера и компонента Центр операций.....	52
Конфигурирование экземпляра сервера.....	52
Установка клиента резервного копирования и архивирования.....	53
Как задать опции для сервера.....	53
Понятия, касающиеся защиты.....	55
Конфигурирование защищенной связи с использованием Transport Layer Security (TLS).....	57
Конфигурирование Центра операций.....	58
Защита связи между компонентом Центр операций и хаб-сервером.....	59
Регистрация лицензии на продукт.....	61
Как задать правила хранения данных для вашего бизнеса.....	61
Как задать расписания для операций по обслуживанию сервера.....	62
Перемещение носителей резервных копий.....	67
Перемещение данных набора хранения в ленточную систему хранения и из нее.....	71
Определение расписаний клиентов.....	78
Подключение ленточных устройств к серверу.....	78
Подключение устройства автоматизированной библиотеки к компьютеру.....	78
Установка режима библиотеки.....	79
Выбор драйвера ленточного устройства.....	79
Драйверы ленточных устройств IBM.....	80
Драйверы ленточных устройств IBM Spectrum Protect.....	80
Специальные имена файлов для ленточных устройств.....	81
Установка и конфигурирование драйверов ленточных устройств.....	82
Установка и конфигурирование драйверов устройств IBM для ленточных устройств IBM.....	83
Системы AIX.....	86
Системы Linux.....	89
Системы Windows.....	92
Конфигурирование библиотек для использования сервером.....	94
Определение ленточных устройств.....	95
Определение библиотек и накопителей.....	95
Описание классов ленточных устройств.....	98
Конфигурирование совместного использования библиотеки.....	105
Пример: совместное использование библиотек для серверов AIX и Linux.....	106
Пример: совместное использование библиотек для серверов Windows.....	108
Настройка иерархии пулов хранения.....	111
Защита приложений и компьютеров.....	112
Добавление клиентов.....	112
Выбор программного обеспечения клиента и планирование установки.....	113
Как задать роли для резервного копирования и архивирования данных клиента.....	115
Планирование операций резервного копирования и архивирования.....	119
Регистрация клиентов.....	120
Установка и настройка клиентов.....	121
Конфигурирование перемещения данных в режиме без сети;.....	125
Проверка конфигурации для использования режима без локальной сети.....	126
Методы шифрования.....	127
Конфигурирование шифрования ленточных накопителей.....	129
Управление операциями ленточного хранения.....	131
Как IBM Spectrum Protect заполняет тома.....	131
Указание оценочной емкости ленточных томов.....	131
Указание формата записей для ленточных носителей.....	132
Как связать объекты библиотеки с классами устройств.....	132
Управление операциями монтирования носителей для ленточных и оптических устройств.....	133
Управление числом одновременно смонтированных томов.....	133
Управление интервалом времени, в течение которого том остается смонтированным..	134
Управление временем ожидания накопителя сервером.....	134
Прерывание операций.....	135

Приоритетное прерывание точки монтирования.....	135
Приоритетное прерывание доступа к тому.....	136
Влияние изменений устройств в SAN.....	136
Вывод сведений об устройстве.....	137
Носители с однократной записью и многократным чтением (WORM).....	137
Накопители, поддерживающие WORM.....	138
Активация носителей WORM.....	138
Ограничения, касающиеся носителей WORM.....	138
Ошибки монтирования при использовании носителей класса WORM.....	139
Изменение меток носителей WORM.....	139
Удаление закрытых томов WORM из библиотеки.....	139
Создание томов DLT WORM.....	139
Поддержка коротких и обычных лент 3592 WORM.....	139
Как запросить в классе устройств информацию о значении параметра WORM.....	140
Устранение ошибок устройств.....	140
Завершение реализации.....	141

Часть 3. Мониторинг..... 143

Ежедневный контрольный список.....	143
Периодический контрольный список.....	155
Мониторинг оповещений ленточных устройств для выявления аппаратных ошибок.....	162
Как избежать ошибок, связанных с несовместимостью носителей.....	163
Операции с чистящими картриджами.....	163
Проверка на соответствие лицензии.....	164
Состояние системы отслеживания с использованием отчетов по электронной почте.....	165

Часть 4. Управление..... 167

Управление Центром операций.....	167
Управление операциями клиентов.....	167
Оценка ошибок в журналах ошибок клиентов.....	167
Остановка и перезапуск приемника клиента.....	168
Изменение паролей.....	169
Управление обновлениями клиентов.....	170
Списание клиентского узла.....	171
Деактивация данных для высвобождения пространства хранения.....	174
Управление системой хранения данных.....	174
Управление емкостью перечня.....	174
Тонкая настройка запланированных операций.....	176
Оптимизация операций путем включения совместного размещения файлов клиентов.....	177
Влияние функции совместного размещения на выполнение операций.....	179
Выбор томов с включенным совместным размещением.....	181
Выбор томов с выключенным совместным размещением.....	183
Параметры совместного размещения.....	184
Совместное размещение пулов хранения копий.....	184
Совместное размещение пулов длительного хранения.....	185
Планирование применения и активизация функции совместного размещения.....	186
Управление ленточными устройствами.....	188
Подготовка сменных носителей.....	188
Запись меток томов на ленточных томах.....	189
Регистрация томов хранения в библиотеке.....	191
Управление перечнем томов.....	196
Управление доступом к томам.....	196
Повторное использование лент.....	196
Поддержание запаса чистых томов.....	198
Поддержание запаса томов в библиотеке, содержащей носители WORM.....	199
Управление перечнем томов в автоматизированных библиотеках.....	199
Частично записанные тома.....	203

Операции совместно используемых библиотек.....	203
Серверные запросы на тома.....	205
Управление ленточными накопителями.....	207
Обновление накопителей.....	207
Отключение ленточных накопителей.....	208
Проверка данных при операциях записи на ленту или чтения с ленты.....	208
Поддерживаемые накопители.....	209
Включение и отключение защиты логических блоков.....	210
Операции чтения/записи для томов.....	211
Управление пулами хранения в ленточной библиотеке.....	212
Очистка ленточных накопителей.....	212
Методы очистки ленточных накопителей.....	212
Конфигурирование сервера для очистки накопителей в автоматизированной библиотеке.....	213
Устранение ошибок, связанных с очисткой накопителей.....	215
Замена ленточного накопителя.....	216
Удаление ленточных накопителей.....	216
Замена накопителей другими накопителями того же типа.....	217
Перенос данных на обновленные накопители.....	217
Защита сервера.....	218
Управление администраторами.....	218
Изменение требований к паролям.....	219
Защита сервера в системе.....	220
Ограничение доступа пользователей к серверу.....	221
Остановка и запуск сервера.....	221
Остановка сервера.....	221
Запуск сервера для задач обслуживания или реконфигурирования.....	222
Планирование обновления сервера.....	223
Подготовка к отключению.....	224
Подготовка к аварии и восстановление после аварии с использованием DRM.....	225
Файл плана аварийного восстановления	225
Восстановление данных сервера и клиента.....	227
Отработка восстановления.....	229
Восстановление базы данных.....	230
Приложение А. Специальные возможности.....	233
Замечания.....	235
Глоссарий.....	239
Индекс.....	241

Об этой публикации

В этой публикации представлена информация о планировании, реализации, мониторинге и работе с решением по защите данных, в котором используются наилучшие практические методы IBM Spectrum Protect.

Для кого предназначено это руководство

Это руководство предназначено для всех пользователей, зарегистрированных как администраторы IBM Spectrum Protect. Решением IBM Spectrum Protect может управлять один администратор, или обязанности администратора могут быть распределены между несколькими людьми.

Для работы с решением необходимо хорошо знать операционную систему сервера и протоколы связи для среды клиента или сервера. Также необходимо понимать принципы управления хранением данных в вашей организации, например, принципы резервного копирования файлов рабочей станции и использования устройств хранения.

Публикации

В семейство продуктов IBM Spectrum Protect входят IBM Spectrum Protect Plus, IBM Spectrum Protect for Virtual Environments, IBM Spectrum Protect for Databases и ряд других продуктов по управлению хранением от IBM®.

Документацию к продуктам IBM смотрите на веб-странице [IBM Knowledge Center](#).

Что нового в этом выпуске

Этот выпуск IBM Spectrum Protect содержит новые функции и обновления.

Список новых функций и обновлений в этом выпуске смотрите в следующих разделах: .

- [Что нового для компонентов сервера](#)
- [Что нового для компонентов клиента](#)

Новая и измененная информация в этой документации по продукту отмечена вертикальной чертой (!) слева от изменения.

Часть 1. Планирование решения защиты данных на основе ленты

Спланируйте решение по защите данных, включающее в себя операции резервного копирования с диска на диск и на ленту и с диска на ленту, чтобы оптимизировать хранение.

Дорожная карта планирования

Запланируйте решение на лентах, ознакомившись со схемой архитектуры в разделе Рисунок 1 на стр. 1, а затем выполнив задачи в дорожной карте, которые приводятся после диаграммы.

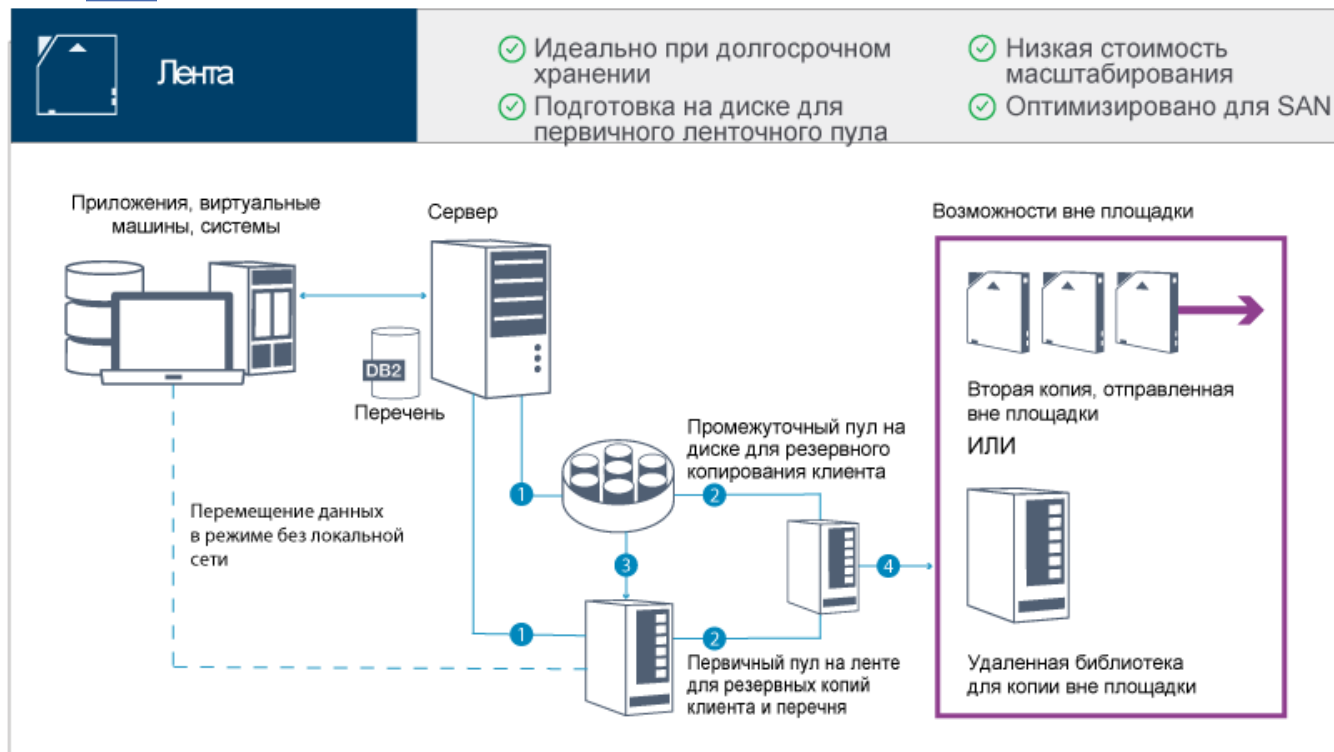


Рисунок 1. Решение на лентах

При такой конфигурации защиты данных сервер использует как дисковое, так и ленточное оборудование для хранения данных. Используется промежуточный пул хранения, когда данные клиентов первоначально сохраняются в дисковых пулах хранения, а потом переносятся в ленточные пулы хранения. Ленточные тома для восстановления после аварий можно хранить вне площадки. Опции вне площадки включают в себя физическое перемещение курьером второй копии вне площадки или электронное хранение копий вне площадки в удаленной библиотеке.

Советы:

- В описанном решении данные *переносятся* из дисковых пулов хранения в ленточные пулы хранения. Однако вместо переноса данных можно использовать функцию tiering-to-tape (разбиение на слои на ленту), введенную в IBM Spectrum Protect версии 8.1.8. Используя эту функцию, можно автоматически разбивать данные на слои из пулов хранения каталогов-контейнеров на диске в ленточную систему хранения. Можно указать, что все данные будут разбиты на слои в соответствии с заданным порогом возраста или что только неактивные данные будут разбиты на слои в зависимости от порога возраста. Дополнительную информацию о том, как данные разбиваются на слои в ленточную систему хранения, смотрите в разделе [Разбиение данных на слои для облачного или ленточной системы хранения](#).

- Описанное решение не включает в себя репликацию узлов. Если вы хотите использовать репликацию узлов, чтобы создать резервную копию пула хранения с диска на диск, убедитесь, что операция репликации завершилась, прежде чем переносить данные с диска на ленту. Репликацию узлов также можно использовать для резервного копирования пула хранения на локальном ленточном устройстве в пул хранения копий на локальном ленточном устройстве.

Чтобы спланировать решение на основе магнитных лент, выполните следующие задачи:

1. Выполните требования к аппаратному и программному обеспечению.
2. Запишите значения конфигурации системы в рабочие листы планирования.
3. Спланируйте дисковое хранение.
4. Спланируйте ленточное хранение.
5. Спланируйте защиту.

Требования к планированию лент

Прежде чем реализовать решение на лентах, ознакомьтесь с общими рекомендациями относительно требований к системе. Определите, нужно ли производить резервное копирование данных на диск и/или на ленту.

Пропускная способность сети

У сети должна быть достаточная пропускная способность, соответствующая ожидаемой передаче данных между клиентом и сервером, и для выполнения операций восстановления с одной площадки на другую, если это требуется для аварийного восстановления. Используйте сеть хранения данных (Storage Area Network, SAN) для передачи данных между сервером, дисковыми устройствами и ленточными устройствами. Дополнительную информацию смотрите в разделе “Требования к аппаратным средствам” на стр. 3.

Перенос данных

Переносите все данные с диска на ленту ежедневно. Задайте для пулов хранения на основе дисков класс устройств FILE. Запланируйте перенос, чтобы управлять тем, когда будет происходить обработка. Чтобы предотвратить автоматический перенос на основе порога переноса, задайте значение 100 для параметра **HIGHMIG** и значение 0 для параметра **LOWMIG**, когда будете вводить команду **DEFINE STGPPOOL**. Вы должны оставить хотя бы 20% ленточных накопителей доступными для операций восстановления. Чтобы использовать до 80% доступных ленточных накопителей и повысить пропускную способность, задайте параметр **MIGPROCESS**.

Учтите следующую информацию, основанную на типе переносимых данных:

- Используйте ленту для резервного копирования данных с клиентов, на которых есть такие большие объекты, как базы данных.

Совет: Обратитесь к производителю ленточных накопителей, чтобы получить рекомендации по размеру базы данных, подходящей для записи на ленту.

- Используйте диск для резервного копирования данных с клиентов, на которых есть объекты меньшего размера.
- Чтобы производить резервное копирование данных непосредственно на ленту, используйте перемещение данных в режиме без локальной сети. Дополнительную информацию смотрите в разделе “Конфигурирование перемещения данных в режиме без сети,” на стр. 125.
- Не производите резервное копирование виртуальных машин на ленту. Используйте отдельный пул хранения на основе дисков, который не переносится в пул хранения на основе лент. Более подробную информацию о поддержке виртуальных машин смотрите в разделе Поддержка гостевой поддержки IBM Spectrum Protect и IBM Tivoli Storage Manager (TSM) для виртуальных машин и виртуализации.

Емкость пула хранения

У вас должна быть достаточная емкость пула хранения, чтобы можно было в течение 2 дней производить резервное копирование клиента, и должно быть 20% для буфера. Возможно, вам придется запланировать полное резервное копирование через несколько дней, чтобы убедиться, что у вас достаточно пространства в пуле хранения.

Ленточные накопители

Ознакомьтесь со спецификациями производителя и оцените емкость ленточного накопителя. Определите объем пространства, который потребуется для выполнения операций резервного копирования и переноса. Зарезервируйте 20% ленточных накопителей для операций восстановления.

Информация, связанная с данной

[MIGRATE STGPOOL \(перенастройка пула хранения в следующий пул хранения\)](#)

Требования к системе для решения на основе ленты

Требования к аппаратному и программному обеспечению представлены для решения по хранению на основе лент со скоростью поглощения данных, равной 14 ТБ в час.

Ознакомьтесь с этой информацией, чтобы узнать о требованиях к аппаратному и программному обеспечению для вашей среды хранения. Возможно, вам придется внести корректировки в зависимости от размера системы.

Требования к аппаратным средствам

Требования к аппаратному обеспечению решения IBM Spectrum Protect основаны на размере системы. Чтобы обеспечить оптимальную производительность среды, выберите компоненты, эквивалентные тем, которые здесь перечислены, либо лучшие компоненты.

Более подробную информацию о планировании дисковых накопителей смотрите в разделе [Планирование дисковой системы хранения](#).

Более подробную информацию о планировании ленточных накопителей смотрите в разделе [Планирование ленточной системы хранения](#).

В следующей таблице приводятся минимальные требования к аппаратному обеспечению для сервера и хранения. Если вы используете локальные разделы (LPAR) или рабочие разделы (WPAR), скорректируйте требования к сети, чтобы учесть размер разделов. Цифры в таблице основаны на скорости поглощения данных, равной 14 ТБ в час.

Аппаратный компонент	Требования к системе
Процессор сервера	<div><div>AIX</div>8 ядер процессора, 3,42 ГГц или быстрее. Например, используйте основанный на процессоре POWER8 сервер.</div> <div><div>Linux</div><div>Windows</div>16 ядер процессора, 2,0 ГГц или быстрее. Например, используйте процессор Intel Xeon.</div>
Память сервера	64 ГБ ОП.

Аппаратный компонент	Требования к системе
Сеть	<p>Указанный ниже размер управляет примерно 14 ТБ данных в час:</p> <ul style="list-style-type: none"> • Ethernet на 10 Гбит (минимум четыре порта) • Адаптер Fibre Channel на 8 Гбит (минимум четыре порта) <p>Число портов зависит от процента ежедневного поглощения данных в дисковые пулы хранения по сравнению с ленточной системой хранения.</p> <p>Используйте отдельные адаптеры Fibre Channel для данных на лентах и дисках.</p>
Хранение	<p>Диск</p> <p>В зависимости от того, какой объем данных вы записываете на диск, укажите нужное вам число дисков.</p> <p>Убедитесь, что пропускная способность последовательного ввода-вывода сети области хранения (storage area network, SAN) совпадает с пропускной способностью ввода-вывода для сети в предыдущей строке.</p> <p>Например, если вам нужно создавать резервные копии 10 ТБ данных в течение четырехчасового окна, пропускная способность будет составлять примерно 700 МБ в секунду. В этом случае серверу потребуется фронтальная сеть (путь с клиента на сервер), поддерживающая минимальную пропускную способность, равную 700 МБ в секунду. Внутренняя SAN (путь с сервера на устройство хранения) также должна поддерживать минимальную пропускную способность, равную 700 МБ в секунду.</p> <p>Чтобы вычислить необходимую скорость диска, используйте следующие формулы:</p> <div data-bbox="505 1073 1169 1220" style="background-color: #f0f0f0; padding: 10px;"> <p>(Общий объем ежедневного поглощения данных - объем ежедневного поглощения данных непосредственно на ленту) (Число часов для ежедневных операций резервного копирования клиента) = Мегабайты поглощения данных на диск в час</p> </div> <div data-bbox="505 1255 1117 1354" style="background-color: #f0f0f0; padding: 10px;"> <p>(Мегабайты поглощения данных на диск в час) ÷ (3600 секунд в час) = Мегабайты поглощения данных в секунду, которые должна поддерживать дисковая технология</p> </div> <p>Лента</p> <p>Выберите ленточную технологию, которая лучше всего соответствует вашим бизнес-требованиям. Например, используйте ленточные накопители IBM Linear Tape-Open (LTO) или IBM TS1150. Убедитесь, что у вас достаточно точек монтирования для операций резервного копирования клиентов и переноса. Более подробную информацию о планировании ленточной системы хранения смотрите в разделе Планирование ленточной системы хранения. Список поддерживаемых ленточных устройств смотрите в разделе IBM для IBM Spectrum Protect.</p> <p>Совет: Чтобы оптимизировать перемещение данных, используйте перемещение данных в режиме без локальной сети.</p>

Аппаратный компонент	Требования к системе
Адаптеры ввода-вывода SAN	Разделите дисковый и ленточный ввод-вывод. Более подробную информацию о выборе адаптера смотрите в документации по аппаратным продуктам Brocade и по решениям хранения IBM Storwize. Диск Используйте хотя бы два адаптера. Лента Используйте хотя бы два адаптера.

Оценка необходимого объема пространства для Центра операций

Требования к аппаратным средствам для Центра операций включены в предыдущую таблицу за исключением пространства базы данных и архивного журнала (перечня), которые используются компонентом Центр операций для удерживания записей для управляемых клиентов.

Если вы не собираетесь устанавливать Центр операций на том же компьютере, что и сервер IBM Spectrum Protect, вы можете оценить требования к системе отдельно. Чтобы вычислить требования к системе для компонента Центр операций, смотрите описание калькулятора требований к системе в документе [техническое замечание 1641684](#).

Управление компонентом Центр операций на сервере IBM Spectrum Protect - это рабочая нагрузка, требующая дополнительного пространства для операций базы данных как на хаб-сервере, так и на всех подчиненных серверах. Объем пространства на хаб-сервере для архивного журнала будет больше, если хаб-сервер осуществляет мониторинг одного или нескольких подчиненных серверов. Прочтите следующие рекомендации, которые позволяют оценить, какой объем пространства потребуется вашему серверу IBM Spectrum Protect.

Пространство базы данных для Центра операций

Компонент Центр операций использует, примерно, 4,4 ГБ пространства базы данных на каждую 1000 клиентов, отслеживаемых на этом сервере. Это вычисление относится как к хаб-серверам, так и к подчиненным серверам в пределах конфигурации.

Например, рассмотрим хаб-сервер с 2000 клиентов, который также управляет тремя подчиненными серверами, на каждом из которых есть 1000 клиентов. Эта конфигурация дает в итоге 5000 клиентов на четырех серверах. Каждому из подчиненных серверов требуется 4,4 ГБ пространства базы данных. Если подчиненные серверы относятся к IBM Spectrum Protect версии 8.1.2 или новее, хаб-серверу потребуется 8,8 ГБ пространства базы данных только для мониторинга своих 2000 клиентов:

$$(4,4 \text{ ГБ} \times 2) = 8,8 \text{ ГБ}$$

Пространство базы данных для управляемых данных

Управляемые данные - это объем защищенных данных, включая объем данных для всех сохраненных версий.

- Для типов клиентов, которые выполняют резервное копирование Всегда инкрементное для оценки общего объема управляемых данных можно использовать приведенную ниже формулу:

$$\text{Фронтальный объем} + (\text{Фронтальный объем} \times \text{Скорость изменений} \times (\text{Срок хранения} - 1))$$

Например, если вы производите резервное копирование 100 ТБ фронтальных данных, используете 30-дневный срок хранения и у вас 5% скорость изменений, вычислите общий объем управляемых данных, используя следующие значения:

$$100 \text{ ТБ} + (100 \text{ ТБ} \times 0,5 \times (30-1)) = \text{Всего } 245 \text{ ТБ управляемых данных}$$

- Для типов клиентов, которые ежедневно выполняют полное резервное копирование для оценки общего объема управляемых данных можно использовать приведенную ниже формулу:

Фронтальное хранение × (1 + скорость изменений)

Например, если вы производите резервное копирование 10 ТБ фронтальных данных, используете 30-дневный срок хранения и у вас 3% скорость изменений, вычислите общий объем управляемых данных, используя следующие значения:

$10 \text{ ТБ} \times 30 \times (1 + 0,03) = 309 \text{ ТБ}$ управляемых данных

Неструктурированные данные, средний размер объекта: 4 МБ

Структурированные данные, средний размер объекта: 128 МБ

Неструктурированные данные, число объектов =

$(245 \text{ ТБ} \times 1024 \times 1024) / 4 \text{ МБ} = 64225280$

Структурированные данные, число объектов =

$(309 \text{ ТБ} \times 1024 \times 1024) / 128 \text{ МБ} = 2531328$

Общее число объектов: 66756608

Затраты на управляемые данные (1 КБ на объект) =

$(66756608 \text{ КБ}) / (1024 \times 1024) = 63,66 \text{ ГБ}$

Запланируйте 20% дополнительного пространства, чтобы системы базы данных не использовались на 100% емкости:

Требования
к общему физическому пространству хранения базы данных =
(управляемое пространство данных + пространство Центра операций) × (1.20)

В этом примере вы вычислите пространство, используя следующие значения:

$(66,33 \text{ ГБ} + 8,4 \text{ ГБ}) \times 1,20 = 76,41 \text{ ГБ}$

Пространство архивного журнала

Центр операций использует, примерно, 18 ГБ пространства архивного журнала каждые 24 часа на каждом сервере для каждой 1000 клиентов на этом сервере. Кроме того, для каждой 1000 клиентов, мониторинг которых осуществляется на подчиненных серверах, на хаб-сервере используется дополнительное пространство архивного журнала. В случае подчиненных серверов версии 8.1.2 или новее этот добавленный объем представляет собой 1,2 ГБ пространства архивного журнала на хаб-сервере на 1000 клиентов, отслеживаемых каждые 24 часа.

Например, рассмотрим хаб-сервер с 2000 клиентов, который также управляет тремя подчиненными серверами, на каждом из которых есть 1000 клиентов. Эта конфигурация дает в итоге 5000 клиентов на четырех серверах. Пространство архивного журнала для хаб-сервера можно вычислить по следующей формуле:

$((18 \text{ ГБ} \times 2) + (1,2 \text{ ГБ} \times 3)) = 39,6 \text{ ГБ}$ пространства архивного журнала

Эти оценки основаны на интервале сбора данных о состоянии по умолчанию, равном 5 минутам. Если вы сократите интервал сбора данных с одного раза за 5 минут до одного раза за 3 минуты, требования к пространству возрастут. В следующих примерах показано примерное увеличение требований к пространству журнала при интервале сбора данных один раз в 3 минуты для конфигурации, в которой производится мониторинг подчиненных серверов V8.1.2 или новее:

- Хаб-сервер: В диапазоне от 39,6 ГБ до 66 ГБ

- Каждый подчиненный сервер: В диапазоне от 18 ГБ до 30 ГБ

Выделите пространство архивного журнала, чтобы вы смогли поддерживать Центр операций, не влияя на операции сервера.

Требования к программному обеспечению

Документация по решению IBM Spectrum Protect на основе лент содержит задачи по установке и конфигурированию для операционных систем IBM AIX, Linux® и Microsoft Windows. У вас должны быть выполнены минимальные требования к программам из перечисленных.

Информацию о требованиях к программам для драйверов ленточных устройств IBM смотрите в разделе [Руководство по установке и использованию IBM Tape Device Drivers](#).

Системы AIX

Тип ПО	Минимальные требования к программному обеспечению
Операционная система	IBM AIX 7.1 Дополнительную информацию о требованиях к операционным системам смотрите в разделе AIX: минимальные требования к системе для систем AIX .
Утилита gunzip	Утилита gunzip должна быть доступна в вашей системе до установки или обновления сервера IBM Spectrum Protect . Убедитесь, что утилита gunzip установлена и ее путь задан в переменной среды PATH.
Тип файловой системы	Файловые системы JFS2 Системы AIX могут кэшировать большие объемы данных файловой системы; при этом может сокращаться объем памяти, необходимый серверу и процессам IBM Db2. Чтобы избежать подкачки при использовании сервера AIX, используйте для файловой системы JFS2 опцию монтирования <code>tbw</code> . Для кэша файловой системы используется меньше памяти, и для IBM Spectrum Protect будет доступно больше памяти. Не используйте опции монтирования файловой системы с параллельным вводом-выводом (Concurrent I/O, CIO) и с прямым вводом-выводом (Direct I/O, DIO) для файловых систем, содержащих журналы базы данных IBM Spectrum Protect или тома пулов хранения. Использование этих опций может вызывать снижение производительности многих серверных операций. IBM Spectrum Protect и Db2 все равно могут использовать DIO там, где это выгодно, но для IBM Spectrum Protect не требуются опции монтирования, чтобы выборочно использовать преимущества этого метода.
Другое программное обеспечение	Оболочка Korn (ksh)

Системы Linux

Тип ПО	Минимальные требования к программному обеспечению
Операционная система	Red Hat Enterprise Linux 7 (x86_64)

Тип ПО	Минимальные требования к программному обеспечению
Библиотеки	Библиотеки GNU C версии 2.3.3-98.38 или новее, устанавливаемые в системе IBM Spectrum Protect. Серверы Red Hat Enterprise Linux: <ul style="list-style-type: none"> • libaio • libstdc++.so.6 (требуется 32- и 64-разрядные пакеты) • numactl.x86_64
Тип файловой системы	Сформатируйте файловые системы, связанные с базами данных, используя ext3 или ext4. Для файловых систем, связанных с пулами, используйте XFS.
Другое программное обеспечение	Оболочка Korn (ksh)

Системы Windows

Тип ПО	Минимальные требования к программному обеспечению
Операционная система	Microsoft Windows Server 2012 R2 (64-разрядная система) или Windows Server 2016
Тип файловой системы	NTFS
Другое программное обеспечение	Должны быть установлены и включены Windows 2012 R2 или Windows 2016 с платформой .NET Framework 3.5. Должны быть отключены следующие политики управления учетными записями пользователей: <ul style="list-style-type: none"> • Управление учетными записями пользователей: Режим Утверждать администраторов для встроенной учетной записи Администратор • Управление учетными записями пользователей: Запускать всех администраторов в режиме Утверждать администраторов

Рабочие листы планирования

Используйте рабочие таблицы планирования, чтобы записывать в них значения, которые вы используете при настройке системы с последующим конфигурированием сервера IBM Spectrum Protect. Используйте наилучшие практические значения по умолчанию, приведенные в рабочих таблицах.

Каждая рабочая таблица поможет вам подготовиться к разным стадиям конфигурирования системы за счет использования наилучших практических значений:

Предварительное конфигурирование серверной системы

Используйте рабочие таблицы предварительного конфигурирования для планирования файловых систем и каталогов, которые вы создадите, когда сконфигурируете файловые системы для IBM Spectrum Protect во время настройки системы. Все каталоги, созданные вами для сервера, должны быть пустыми.

Конфигурация сервера

Воспользуйтесь рабочими таблицами по конфигурированию, когда будете конфигурировать сервер. Для большинства элементов предлагаются значения по умолчанию, кроме случаев, когда это отмечено.

Таблица 1. Рабочая таблица для предварительного конфигурирования серверной системы				
Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Дополнительная информация
Адрес порта TCP/IP для взаимодействия с сервером	1500		Неприменимо.	Убедитесь, что этот порт доступен, когда будете устанавливать и конфигурировать операционную систему. Номер порта может быть числом в диапазоне от 1024 до 32767.
Каталог для экземпляра сервера	<div>Linux AIX</div> /home/tsminst1/tsminst1 <div>Windows</div> C:\tsminst1		<div>AIX</div> 50 ГБ. <div>Linux Windows</div> 25 ГБ.	Если вы измените значение каталога экземпляра сервера по сравнению со значением по умолчанию, измените также значение владельца экземпляра Db2 в Таблица 2 на стр. 11 .
Каталог для установки сервера	<ul style="list-style-type: none"> <div>Linux AIX</div> / <div>Windows</div> C: 		<div>AIX</div> Доступное пространство, необходимое для каталога: 5 ГБ. <div>Linux Windows</div> Минимальное пространство, необходимое для каталога: 30 ГБ	
Каталог для установки сервера	/usr		<div>AIX</div> Доступное пространство, необходимое для каталога: 5 ГБ.	
Каталог для установки сервера	<div>AIX</div> /var		<div>AIX</div> Доступное пространство, необходимое для каталога: 5 ГБ.	

Таблица 1. Рабочая таблица для предварительного конфигурирования серверной системы (продолжение)				
Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Дополнительная информация
Каталог для установки сервера	AIX /tmp		AIX Доступное пространство, необходимое для каталога: 5 ГБ.	
Каталог для установки сервера	AIX /opt		AIX Доступное пространство, необходимое для каталога: 10 ГБ.	
Каталог для активного журнала	Linux AIX / tsminst1/TSMalog Windows C:\tsminst1\TSMalog		128 ГБ.	Если вы создаете активный журнал при первоначальном конфигурировании сервера, задайте размер, равный 128 ГБ.
Каталог для архивного журнала	Linux AIX / tsminst1/TSMarchlog Windows C:\tsminst1\TSMarchlog		3 ТБ.	
Каталоги для базы данных	Linux AIX /tsminst1/TSMdbspace00 /tsminst1/TSMdbspace01 /tsminst1/TSMdbspace02 /tsminst1/TSMdbspace03 Windows C:\tsminst1\TSMdbspace0 0 C:\tsminst1\TSMdbspace0 1 C:\tsminst1\TSMdbspace0 2 C:\tsminst1\TSMdbspace0 3		Инструкции по вычислению требований пространства смотрите в разделе “Требования к аппаратным средствам” на стр. 3.	Создайте четыре файловых системы для базы данных.

Таблица 1. Рабочая таблица для предварительного конфигурирования серверной системы (продолжение)				
Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Дополнительная информация
Каталоги для хранения	<div>Linux AIX</div> /tsminst1/TSMfile00 /tsminst1/TSMfile01 /tsminst1/TSMfile02 /tsminst1/TSMfile03 ... <div>Windows</div> C:\tsminst1\TSMfile00 C:\tsminst1\TSMfile01 C:\tsminst1\TSMfile02 C:\tsminst1\TSMfile03 ...		Определите минимальную общую емкость для всех каталогов, используя следующее вычисление: <div>Ежедневный процент принятых данных, записанных на диск + 20% = Минимальная общая емкость</div>	Предпочтительный метод - задать хотя бы один каталог для каждого ленточного устройства.

Таблица 2. Рабочая таблица для конфигурирования IBM Spectrum Protect			
Элемент	Значение по умолчанию	Собственное значение	Дополнительная информация
Владелец экземпляра Db2	tsminst1		Если вы изменили значение по умолчанию для каталога экземпляра сервера в таблице Таблица 1 на стр. 9 , то измените также значение владельца экземпляра Db2.
Пароль владельца экземпляра Db2	<div>Linux AIX</div> passw0rd <div>Windows</div> pAssW0rd		Выберите в качестве пароля владельца экземпляра значение, отличающееся от значения по умолчанию. Обязательно запишите это значение и храните его в надежном месте.
Первичная группа для владельца экземпляра Db2	<div>Linux AIX</div> tsmsrvrs		
Имя сервера	Значением по умолчанию для имени сервера является системное имя хоста.		

Таблица 2. Рабочая таблица для конфигурирования IBM Spectrum Protect (продолжение)			
Элемент	Значение по умолчанию	Собственное значение	Дополнительная информация
Пароль сервера	passw0rd		Выберите в качестве пароля сервера значение, отличающееся от значения по умолчанию. Обязательно запишите это значение и храните его в надежном месте.
ID администратора: ID пользователя для экземпляра сервера	admin		
Пароль ID администратора	passw0rd		Выберите в качестве пароля администратора значение, отличающееся от значения по умолчанию. Обязательно запишите это значение и храните его в надежном месте.

Таблица 2. Рабочая таблица для конфигурирования IBM Spectrum Protect (продолжение)

Элемент	Значение по умолчанию	Собственное значение	Дополнительная информация
Плановое время начала	23:00		<p>Время начала расписания по умолчанию соответствует началу фазы рабочей нагрузки клиента, которая преимущественно состоит из операций резервного копирования и архивирования клиента. Во время фазы рабочей нагрузки клиента ресурсы сервера поддерживают операции клиента. Обычно эти операции завершаются в течение окна ночного расписания.</p> <p>Расписания для операций по обслуживанию сервера заданы так, чтобы они начинались через 10 часов после начала окна резервного копирования клиента.</p> <p>В этом руководстве рекомендуемое время для запуска операций резервного копирования клиента - 23:00.</p>

Таблица 3. Рабочий лист для ленточного конфигурации			
Элемент	Значение по умолчанию	Собственное значение	Дополнительная информация
Файлы роботизированных устройств	<p>Устройства IBM с драйвером ленточных устройств IBM:</p> <ul style="list-style-type: none"> • AIX /dev/smcX • Linux /dev/IBMchangerX • Windows ChangerX <p>Устройства не IBM с драйвером устройств IBM Spectrum Protect:</p> <ul style="list-style-type: none"> • AIX /dev/lbX • Linux /dev/tsm SCSI/lbX • Windows lbA.B.C.D 		<p>Чтобы вручную задать файлы устройств библиотеки, используйте следующие команды:</p> <ul style="list-style-type: none"> • DEFINE LIBRARY • DEFINE DRIVE • DEFINE PATH <p>Для SCSI можно использовать команду PERFORM LIBACTION, чтобы задать все накопители и их пути для одной библиотеки за один шаг. Чтобы использовать эту команду для назначения всех накопителей и путей, нужно, чтобы поддерживалась и была включена опция SANDISCOVERY.</p>
Ленточные накопители	<p>Устройства IBM с драйвером ленточных устройств IBM:</p> <ul style="list-style-type: none"> • AIX /dev/rmtX • Linux /dev/IBMTapeX • Windows TapeX <p>Устройства не IBM с драйвером устройств IBM Spectrum Protect:</p> <ul style="list-style-type: none"> • AIX /dev/mtX • Linux /dev/tsm SCSI/mtX • Windows mtA.B.C.D 		

Планирование дисковой системы хранения

Выберите наиболее эффективную технологию хранения для компонентов IBM Spectrum Protect, чтобы обеспечить эффективную работу сервера и высокую производительность операций.

У аппаратных устройств хранения разные характеристики емкости и производительности, что определяет то, как их можно эффективно использовать вместе с IBM Spectrum Protect. Общие

рекомендации по выбору соответствующего оборудования хранения и настройке вашего решения смотрите в указанных ниже источниках.

База данных, активный журнал и архивный журнал

- Используйте твердотельный диск (SSD) или быстрый диск на 15000 об/мин для базы данных и активного журнала IBM Spectrum Protect.
- При создании массивов для базы данных используйте RAID уровня 5.
- Используйте отдельные диски для хранения резервной копии базы данных и архивного журнала.

Пул хранения

Используйте RAID уровня 6 для массивов пулов хранения, чтобы добавить защиту от двойных сбоев диска при использовании крупных типов дисков.

Планирование массивов хранения

Подготовьтесь к конфигурированию дискового хранения, спланировав массивы RAID и тома в соответствии с размером вашей системы IBM Spectrum Protect.

Вы разрабатываете массивы хранения, размер и характеристики производительности которых подходят для одного из компонентов серверной системы хранения IBM Spectrum Protect, например, базы данных сервера или пула хранения. Операция планирования хранения должна учитывать тип накопителя, уровень RAID, число накопителей, число запасных накопителей и т.п. В конфигурациях решения группы хранения содержат массивы RAID внутреннего хранения, которые состоят из нескольких физических дисков, представленных в системе в виде логических томов. При конфигурировании дисковой системы хранения вы создаете группы хранения или пулы хранения данных, а затем создаете массивы хранения в группах.

Вы создаете тома или LUN из групп хранения. Группа хранения задает, какие диски обеспечивают пространство хранения, составляющее том. При создании томов сделайте их полностью выделенными. Используются более быстрые типы дисков, чтобы хранить тома базы данных и активные тома журнала. Более медленные типы дисков можно использовать для томов пула хранения, архивного журнала и томов резервных копий базы данных. Если для подготовки данных используется меньший пул хранения на основе дисков, вам, возможно, придется использовать более быстрые диски, чтобы справиться с ежедневной рабочей нагрузкой по поглощению и перенастройке данных.

В разделах [Таблица 4 на стр. 15](#) и [Таблица 5 на стр. 16](#) описаны требования к схеме для конфигурации групп хранения и томов.

<i>Таблица 4. Компоненты конфигурации группы хранения</i>	
Компонент	Подробности
Требования к пространству хранения на сервере	Как сервер использует пространство хранения.
Тип диска	Размер и скорость для типа диска, используемого в соответствии с требованиями хранения.
Количество дисков	Число дисков каждого типа, которые необходимы в соответствии с требованиями к хранению.
Емкость горячего резервирования	Число дисков, зарезервированных в качестве запасных для передачи управления в случае отказа диска.
Уровень RAID	Уровень массива RAID, используемый для логического хранения. Уровень RAID определяет тип избыточности, обеспечиваемой массивом, например 5 или 6.

Таблица 4. Компоненты конфигурации группы хранения (продолжение)	
Компонент	Подробности
Количество массивов RAID	Количество создающихся массивов RAID.
DDM на массив RAID	Сколько модулей дисководов (disk drive module, DDM) нужно использовать в каждом из массивов RAID.
Используемый размер на массив RAID	Размер пространства, доступный для хранения данных в каждом массиве RAID после вычета пространства, потерянного вследствие избыточности.
Общий используемый размер	Общий размер, доступный для хранения данных в массивах RAID: Количество x Используемый размер
Рекомендуемые имена групп хранения и массивов	Предпочтительное имя, которое следует использовать для дисков MDisk и групп MDisk.
Использование	Компонент сервера, который использует часть физического диска.

Таблица 5. Компоненты конфигурации томов	
Компонент	Подробности
Требования к пространству хранения на сервере	Требования, в соответствии с которыми используется физический диск.
Имя тома	Уникальное имя, присвоенное отдельному тому.
Группа хранения	Имя группы хранения, для которой будет взято пространство, чтобы создать том.
Размер	Размер каждого тома.
Предполагаемая точка монтирования сервера	Каталог на компьютере сервера, где монтируется том.
Количество	Число томов, которые нужно создать для выполнения определенных требований. Используйте один и тот же стандарт присвоения имен для каждого тома, созданного в соответствии с теми же требованиями.
Использование	Компонент сервера, который использует часть физического диска.

Примеры

Примеры конфигурации для групп хранения и томов можно найти, воспользовавшись следующей ссылкой: [Примеры рабочих листов для планирования массивов хранения](#). В примерах показано, как спланировать хранение при разных размерах серверов. В конфигурациях примеров существует отображение один на один между дисками MDisk и группами storage. Можно скачать примеры и изменить рабочие листы, чтобы спланировать конфигурацию хранения для сервера.

Планирование ленточной системы хранения

Определите, какие ленточные устройства нужно использовать и как их сконфигурировать. Чтобы оптимизировать производительность системы, запланируйте использование быстрых ленточных

устройств с высокой мощностью. Предоставьте достаточно ленточных накопителей, чтобы их число удовлетворяло вашим бизнес-требованиям.

Поддерживаемые ленточные устройства и библиотеки

Сервер может использовать широкий диапазон ленточных устройств и библиотек. Выберите ленточные устройства и библиотеки, соответствующие вашим бизнес-требованиям.

Список поддерживаемых устройств и допустимых форматов классов устройств смотрите на веб-сайте для вашей операционной системы:

- **AIX** | **Windows** [Поддерживаемые устройства для AIX и Windows](#)
- **Linux** [Поддерживаемые устройства для Linux](#)

Дополнительные сведения об устройствах хранения и объектах хранения смотрите в разделе [Типы устройств хранения](#).

Каждое устройство, определенное для IBM Spectrum Protect, связывается с одним *классом устройств*. Каждый класс устройств задает информацию о типе устройств и управлении носителями, такую как формат записи, оценка емкости и префиксы маркировки.

Тип устройства определяет устройство как элемент группы устройств со схожими параметрами носителей. Например, тип устройств LTO применим ко всем поколениям ленточных накопителей LTO.

Класс устройств для ленточного накопителя должен задавать также библиотеку. *Физическая библиотека* представляет собой набор из одного или нескольких накопителей со схожими требованиями к монтированию носителей. То есть, накопитель может монтироваться оператором или механизмом автоматического монтирования.

Определение объекта библиотеки задает тип библиотеки и другие характеристики, связанные с этим типом библиотеки.

В следующей таблице перечислены предпочтительные типы библиотек для решения на лентах IBM Spectrum Protect версии 8.1.6.

Таблица 6. Типы библиотек для решения на лентах IBM Spectrum Protect 8.1.6

Тип библиотеки	Описание	Дополнительная информация
SCSI	<p>Библиотека SCSI управляется с помощью интерфейса SCSI, подключенного либо непосредственно к хосту сервера с помощью кабелей SCSI, либо через сеть хранения данных. Монтирование и размонтирование ленточных томов автоматически выполняется роботом или другим механизмом.</p> <p>Если вы создадите другие типы накопителей для библиотеки SCSI, вы создадите несколько логических библиотек, которые нельзя разбить между разными типами накопителей. Библиотека SCSI может содержать накопители смешанных технологий, включая LTO Ultrium и накопители цифровых линейных лент (digital linear tape, DLT). Например:</p> <ul style="list-style-type: none"> Библиотека Oracle StorageTek L700 Ленточное устройство IBM 3592 	<p>“Конфигурирование библиотек для использования сервером” на стр. 94</p> <p>Ограничения применяются, если вы смешаете разные поколения носителей и накопителей. Дополнительные сведения смотрите в разделе:</p> <ul style="list-style-type: none"> “Использование носителей 3592 разных поколений в одной библиотеке” на стр. 102 “Использование разных поколений накопителей и устройств LTO в библиотеке” на стр. 99
Совместная	<p>Совместно используемые библиотеки - это логические библиотеки, представленные SCSI. Библиотека управляется сервером IBM Spectrum Protect, настроенным как менеджер библиотеки.</p> <p>Серверы IBM Spectrum Protect, на которых используется тип библиотек SHARED, являются клиентами библиотеки по отношению к серверу менеджера библиотеки. Совместно используемые библиотеки ссылаются на менеджер библиотеки.</p>	

Поддерживаемые конфигурации ленточных устройств

Ознакомьтесь с информацией о локальных сетях (Local Area Network, LAN) и сетях областей хранения данных (storage area network, SAN). Чтобы оптимизировать перемещение данных, запланируйте конфигурирование перемещения данных в режиме без локальной сети. Кроме того, рассмотрите возможность совместного использования библиотек.

Выберите конфигурацию устройства, которая соответствует вашим бизнес-требованиям.

Перемещение данных в режиме с сетью и в режиме без сети

Вы можете перемещать данные между клиентами и устройствами хранения, подключенными к локальной сети (local area network, LAN) или к устройствам хранения, подключенными к сети хранения данных (storage area network, SAN); это называется перемещением данных без локальной сети.

В обычной конфигурации LAN одна или несколько ленточных библиотек связаны с одним сервером IBM Spectrum Protect. Перемещение данных без локальной сети делает ширину полосы пропускания локальной сети доступной для других видов использования и снижает нагрузку на сервер IBM Spectrum Protect.

В конфигурации локальной сети клиентские данные, электронная почта, терминальные подключения, приложение и информация для управления устройствами должны обслуживаться одной и той же сетью. Информация для управления устройством и клиентские данные резервного копирования и восстановления передаются по локальной сети.

Сеть хранения данных (SAN) - это выделенная сеть хранения, которая может дать выигрыш в производительности системы.

Применяя IBM Spectrum Protect в SAN, вы используете преимущества следующих функций:

- Совместно использовать устройства хранения на нескольких серверах IBM Spectrum Protect.

Ограничение: Устройство хранения с типом устройства GENERICTAPE не может совместно использоваться серверами.

- Переместить данные клиента IBM Spectrum Protect непосредственно на устройства хранения (перемещение в режиме без локальной сети), сконфигурировав агент хранения в системе клиента.

В SAN можно совместно использовать ленточные устройства и библиотеки, поддерживаемые сервером IBM Spectrum Protect, в том числе большинство ленточных устройств SCSI.

Когда серверы IBM Spectrum Protect совместно используют ленту SCSI, один сервер, *менеджер библиотек*, владеет устройством и управляет им. Агенты хранения, вместе с другими серверами IBM Spectrum Protect, совместно использующими эту библиотеку - это *клиенты библиотек*. Клиент библиотеки запрашивает совместно используемые ресурсы библиотеки, например, накопители или носители, у менеджера библиотеки, но использует ресурсы независимо. Менеджер библиотеки координирует доступ к этим ресурсам. Серверы IBM Spectrum Protect, определенные как клиенты библиотек, используют связи сервер-сервер для обращения к менеджеру библиотек и для требований служб устройств. Данные перемещаются по сети SAN между каждым сервером и устройством хранения.

Требование: Если вы зададите сервер менеджера библиотеки, который используется совместно с сервером IBM Spectrum Protect, для опции **SANDISCOVERY** нужно задать значение ON. По умолчанию для этой опции задано значение OFF.

Серверы IBM Spectrum Protect при совместном использовании автоматизированной библиотеки задействуют следующие функции:

Разбиение перечня томов

Перечень томов носителей в совместно используемой библиотеке разделяется между серверами. Том либо принадлежит отдельному серверу, либо находится в глобальном чистом пуле. Чистый пул не принадлежит ни одному серверу.

Последовательный доступ к накопителям

К каждому ленточному накопителю одновременно может обращаться только один сервер. Доступ к накопителям сериализован. IBM Spectrum Protect управляет доступом к накопителям, так чтобы серверы не размонтировали тома других серверов и не записывали данные на накопители, где другие серверы могут смонтировать свои тома.

Последовательный доступ для монтирования

Авточейнджер библиотеки одновременно выполняет только одну операцию монтирования или размонтирования. Для обеспечения этой сериализации все операции монтирования выполняются одним сервером (менеджером библиотек).

Совместное использование библиотек

Вы можете оптимизировать эффективность вашего решения на лентах, сконфигурировав совместное использование библиотек. Совместное использование библиотек позволяет нескольким серверам IBM Spectrum Protect использовать одну и ту же ленточную библиотеку и накопители в сети хранения (SAN, storage area network), повышая производительность резервного копирования и восстановления и уровень использования ленточного оборудования.

При совместном использовании библиотеки на серверах IBM Spectrum Protect один сервер, сконфигурированный как менеджер библиотеки, управляет такими операциями библиотеки, как

монтаж и демонтаж. Кроме того, менеджер библиотеки управляет правами собственности на тома и перечнем библиотеки. Остальные серверы, сконфигурированные как клиенты библиотеки, используют связь сервер-сервер для связи с менеджером библиотеки и запроса на использование ресурсов.

Клиенты библиотеки должны иметь такой же уровень версии, как у сервера - менеджера библиотеки, или более ранний. Менеджер библиотеки не может поддерживать клиентов библиотеки с более новым уровнем версии. Более подробную информацию смотрите в разделе [Совместимость агента хранения и библиотечного клиента с сервером IBM Spectrum Protect](#).

перемещение данных в режиме без сети (LAN-free data movement)

IBM Spectrum Protect позволяет клиенту с помощью агента хранения выполнять резервное копирование и восстановление данных непосредственно в ленточную библиотеку в сети SAN. Этот тип перемещения данных также называют перемещением данных в режиме без локальной сети.

Ограничение: Устройства хранения Centera не могут быть объектами назначения для операций в режиме без локальной сети.

На [Рисунок 2 на стр. 20](#) показана конфигурация сети SAN, в которой клиент получает непосредственный доступ к ленте для чтения или записи данных.



Рисунок 2. перемещение данных в режиме без сети (LAN-free data movement)

Перемещение данных в режиме без локальной сети требует установки агента хранения на клиентской системе. Сервер поддерживает базу данных и журнал восстановления и выступает в роли менеджера библиотеки для управления операциями устройства. Агент хранения на клиенте

обрабатывает перенос данных на устройство в сети SAN. Такая реализация освобождает локальную сеть, которая в другом случае использовалась бы для перемещения клиентских данных.

Смешанные типы устройств в библиотеке

IBM Spectrum Protect поддерживает использование разных типов устройств в одной автоматизированной библиотеке, если библиотека может распознавать различные носители для разных типов устройств. Чтобы упростить процесс конфигурирования, не планируйте комбинирование разных типов устройств в библиотеке. Если вам нужно скомбинировать типы устройств, ознакомьтесь с ограничениями.

Библиотеки с этой возможностью - это модели со встроенными смешанными дисками или модели, поддерживающие добавление смешанных дисков. Информацию о конкретных моделях смотрите в документации производителя. Чтобы узнать о библиотеках, протестированных с IBM Spectrum Protect при использовании смешанных типов устройств, смотрите информацию для своей операционной системы:

- [IBM Spectrum Protect: Поддерживаемые устройства для AIX, HP-UX, Solaris и Windows](#)
- [IBM Spectrum Protect: Поддерживаемые устройства для Linux](#)

Например, в одной библиотеке, заданной для сервера IBM Spectrum Protect, у вас могут быть накопители LTO Ultrium и накопители IBM TS4500.

Разные поколения носителей в библиотеке

Сервер IBM Spectrum Protect позволяет использовать устройства разных типов в автоматизированной библиотеке, но использование устройств одного типа, но разных поколений, в общем случае не поддерживается. Новые накопители не могут записывать данные на носители более ранних форматов, а устаревшие накопители не могут считывать данные новых форматов. Исключением из этого правила являются накопители LTO Ultrium.

Если технология, используемая в новом накопителе, не позволяет записывать данные на носители, отформатированные с помощью устройств более раннего поколения. Во избежание проблем с операциями на сервере более ранние носители должны быть обозначены как предназначенные только для чтения. Кроме того, более старые накопители нужно удалить из библиотеки, или нужно удалить определения более старых накопителей с сервера. Например, сервер IBM Spectrum Protect не поддерживает использование накопителей Oracle StorageTek 9940 A с накопителями 9940B в сочетании с другими типами устройств в одной библиотеке.

В общем случае, IBM Spectrum Protect не поддерживает смешение поколений накопителей и носителей LTO Ultrium. Однако поддерживаются следующие комбинации:

- LTO Ultrium поколения 3 (LTO-3) с LTO Ultrium поколения 4 (LTO-4)
- LTO Ultrium поколения 4 (LTO-4) с LTO Ultrium поколения 5 (LTO-5)
- LTO Ultrium поколения 5 (LTO-5) с LTO Ultrium поколения 6 (LTO-6)
- LTO Ultrium поколения 6 (LTO-6) с LTO Ultrium поколения 7 (LTO-7)
- Носители LTO Ultrium поколения 7 (LTO-7) с носителем LTO Ultrium поколения 8 (LTO-8 и LTO-M8) в библиотеке с ленточными накопителями LTO-8 или библиотекой с ленточным накопителем LTO-8 и LTO-7

Сервер поддерживает эти сочетания, поскольку разные накопители могут считывать и записывать данные на различные носители. Если вы собираетесь обновить все накопители до поколения 4 (либо поколения 5, 6, 7 или 8), вы должны удалить все существующие определения накопителей LTO Ultrium и связанные с ними пути. После этого вы можете задать новые накопители и пути для накопителей поколения 4 (либо поколения 5, 6, 7 или 8).

Ограничения, применимые к смешению ленточных накопителей и носителей LTO Ultrium

- Накопители LTO-5 могут читать только носители LTO-3. Если в одной библиотеке одновременно используются накопители и носители LTO-3 с накопителями и носителями LTO-5, вы должны пометить носитель LTO-3 как доступный только для чтения. Нужно резервировать все чистые тома LTO-3.

- Накопители LTO-6 могут читать только носители LTO-4. Если в одной библиотеке одновременно используются накопители и носители LTO-4 с накопителями и носителями LTO-6, вы должны пометить носитель LTO-4 как доступный только для чтения. Нужно зарезервировать все чистые тома LTO-4.
- Накопители LTO-7 могут читать только носители LTO-5. Если в одной библиотеке одновременно используются накопители и носители LTO-5 с накопителями и носителями LTO-7, вы должны пометить носитель LTO-5 как доступный только для чтения. Нужно зарезервировать все чистые тома LTO-5.
- Накопители LTO-8 не могут читать носители LTO-6. Если вы смешиваете накопители и носители LTO-6 с накопителями и носителями LTO-8 в одной библиотеке, вы должны разбить библиотеку на две библиотеки. В одной библиотеке должны быть только накопители и носители LTO-8, а в другой - только накопители и носители LTO-6.

Ограничения, применимые к смешению поколений ленточных накопителей LTO Ultrium в библиотеке

Нужно использовать ленточные картриджи, относящиеся к более раннему поколению, чем ленточный накопитель. Ленточный накопитель более нового поколения может читать данные с ленточных картриджей более раннего поколения и может записывать на них данные. Например, если в библиотеке есть ленточные накопители LTO-7 и LTO-6, нужно использовать ленточные картриджи LTO-6. Как ленточные накопители LTO-7, так и ленточные накопители LTO-6 могут читать данные с ленточных картриджей LTO-6 и могут записывать на них данные.

Ограничения, применимые к смешению поколений ленточных картриджей LTO Ultrium в библиотеке

Следует использовать ленточный картридж, относящийся к тому же поколению, что и ленточный накопитель, или более ранний на одно поколение. Например, если в библиотеке есть ленточные накопители LTO-7, можно использовать ленточные картриджи LTO-7 или комбинацию ленточных картриджей LTO-7 и LTO-6. Если в этой библиотеке есть ленточные картриджи LTO-7, LTO-6 и LTO-5, нужно изменить режим доступа на READONLY для ленточных картриджей LTO-5.

Чтобы узнать о дополнительных замечаниях, связанных с использованием разных поколений LTO Ultrium, смотрите раздел [“Как задать классы устройств LTO”](#) на стр. 99.

При использовании IBM Spectrum Protect нельзя смешивать накопители поколений 3592, TS1130, TS1140, TS1150 и новее. Используйте одну из трех особых конфигураций. Дополнительные сведения смотрите в разделе [“Как задать классы устройств 3592”](#) на стр. 102.

Если в библиотеке будет выполняться шифрование томов, не используйте носители разных поколений в библиотеке.

Носители разных типов в пулах хранения

Вы можете оптимизировать эффективность вашего решения на лентах, не смешивая форматы данных в пуле хранения. Вместо смешения форматов отобразите каждый уникальный формат данных в отдельный пул хранения, используя его собственный класс устройств. Это ограничение также относится к форматам LTO.

Несколько пулов хранения и их классы устройств разных типов могут указывать на одну библиотеку, поддерживающую их, как описано в разделе [“Разные поколения носителей в библиотеке”](#) на стр. 21.

Можно выполнить переход на тип носителей нового поколения в пределах одного пула хранения, выполнив следующие шаги:

1. Замените в библиотеке все более старые накопители на накопители более нового поколения. Накопители должны комбинироваться.
2. Пометьте существующие тома с более старым форматом как тома только для чтения, если новый накопитель не может добавить эти ленты в старом формате. Если новый диск может записывать данные на существующие носители старого формата, это действие можно пропустить. Однако все равно необходимо выполнить шаг 1. Если это необходимо, чтобы оставить в одной и той же библиотеке разные поколения накопителей, которые совместимы по

чтению, но несовместимы по записи, используйте для каждого из них отдельные пулы хранения.

Определения, необходимые для ленточных устройств хранения

Перед тем как сервер IBM Spectrum Protect сможет использовать ленточное устройство, оно должно быть сконфигурировано для операционной системы и для сервера. Как часть процесса планирования, решите, какие определения требуются для ваших накопителей на магнитной ленте.

Совет: Команду **PERFORM LIBACTION** можно использовать для упрощения процесса, когда вы добавляете устройства в типы библиотек SCSI и VTL.

В Таблица 7 на стр. 23 содержится сводка определений, необходимых для различных типов устройств.

Таблица 7. Определения, необходимые для устройств хранения					
Устройство	Типы устройств	Необходимые определения			
		Библиотека	Накопитель	Путь	Класс устройств
Магнитный диск	DISK	—	—	—	Да ¹
	FILE ²	—	—	—	Да
	<div>AIX Windows</div> CENTERA <div>Linux</div> CENTERA ³	—	—	—	Да
Лента	3590 3592 DLT LTO NAS VOLSAFE <div>AIX Windows</div> GENERICTAPE ECARTRIDGE ⁴	Да	Да	Да	Да
Сменный носитель (файловая система)	REMOVABLEFILE	Да	Да	Да	Да

1. Класс устройств DISK присутствует при установке и не может быть изменен.
2. Библиотеки FILE, накопители и пути необходимы для совместного использования с агентами хранения.
3.

Linux

 Тип устройств CENTERA доступен только для систем Linux x86_64.
4. Тип устройств ECARTRIDGE предназначен для накопителей с ленточными картриджами Oracle StorageTek, например, для накопителей 9840 и T10000.

Планирование иерархии пулов хранения

Спланируйте иерархию пулов хранения, чтобы ежедневно производился перенос данных с диска на ленту. При переносе высвобождается пространство на дисковом устройстве, и данные перемещаются на ленту для долгосрочного хранения. Это позволит вам воспользоваться

преимуществами масштабируемости, экономической эффективности и функций защиты ленточной системы хранения.

Прежде чем начать

Иерархия пулов хранения помогает управлять потоком данных. Чтобы понять этот поток данных, ознакомьтесь с [Рисунок 3 на стр. 24](#).

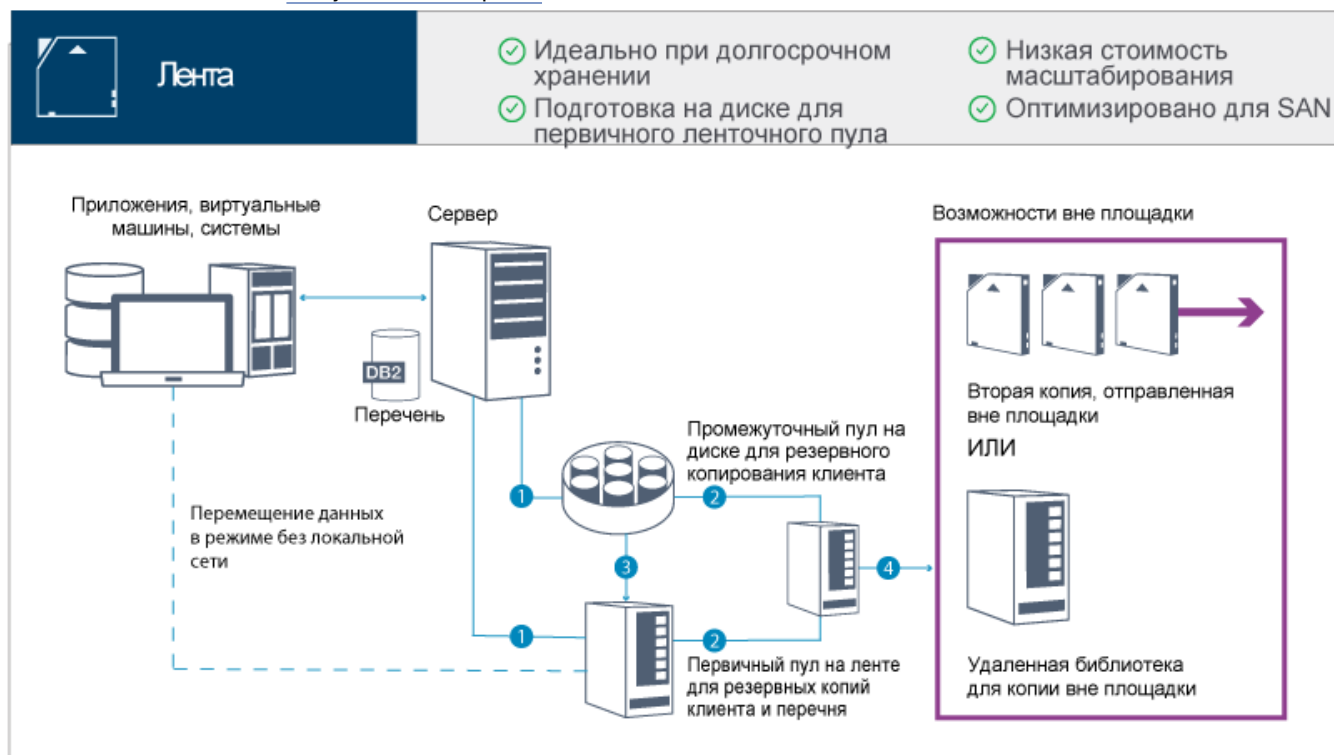


Рисунок 3. Решение на лентах

Следующие шаги соответствуют номерам на рисунке:

1. Сервер получает данные с клиентов (из приложений, с виртуальных машин или из систем) и сохраняет данные в первичных пулах хранения. В зависимости от типа клиента данные хранятся в первичном пуле хранения на диске или на ленте.
2. Производится резервное копирование данных на диск и на ленту в пул хранения копий на ленте.
3. Данные в первичном пуле хранения на диске ежедневно переносятся в первичный пул хранения на ленту.
4. Данные из пула хранения копий на ленте перемещаются куда-либо вне площадки, чтобы обеспечить поддержку долгосрочного хранения и аварийного восстановления.

Процедура

Чтобы спланировать иерархию пулов хранения, ответьте на следующие вопросы:

- а. Какие клиенты должны производить резервное копирование данных на диск и какие клиенты должны производить резервное копирование данных на ленту?
 - Предпочтительный метод - резервное копирование клиентов, на которых находятся большие объекты, например, базы данных, на ленту.
 - Предпочтительный метод - резервное копирование всех остальных клиентов на диск.
 - Для клиентов виртуальных машин (VM) можно производить резервное копирование данных на диск или на ленту. Предпочтительный метод - резервное копирование клиента VM в отдельный дисковый пул хранения, который не переносится на ленту. Если вам нужно

перенести клиент VM на ленту, создайте меньший дисковый пул хранения, чтобы на нем находились файлы управления VMware. Для этого меньшего дискового пула хранения нельзя разрешать перенос на ленту. Дополнительную информацию о резервном копировании клиента VM на ленту смотрите в разделах [Рекомендации по ленточным устройствам](#) и [Поддержка гостевой поддержки IBM Spectrum Protect и IBM Tivoli Storage Manager \(TSM\) для виртуальных машин и виртуализации](#).

Совет: Если многим клиентам приходится копировать данные в один пул хранения, рассмотрите возможность использовать пул хранения на диске, так как вы сможете задать много точек монтирования. Вы сможете задать максимальное значение, равное 999, для параметра **MAXNUMMP** в команде **REGISTER NODE**.

- b. Что следует учесть при назначении емкости пулов хранения на основе диска?

Как минимум, запланируйте достаточную емкость, чтобы хранить данные за один день операций резервного копирования. Предпочтительный метод - запланировать достаточно емкости, чтобы хранить данные за два дня операций резервного копирования, плюс 20% буфер.

- c. Что следует учесть при назначении класса устройств для пула хранения на основе диска?

Предпочтительный метод - задать класс устройств FILE. Задайте для параметра **MOUNTLIMIT** значение 4000. Также убедитесь, что у узла достаточно высокое число точек монтирования, которые можно задать, используя параметр **MAXNUMMP** в команде **REGISTER NODE**.

- d. Нужно ли задавать дедупликацию данных для дискового пула хранения?

Нет, так как данные хранятся на диске в течение только одного дня, прежде чем данные переносятся на ленту.

- e. Следует ли задавать автоматический перенос данных на основе порога переноса?

Нет. Вместо этого запланируйте ежедневный перенос, используя команду **MIGRATE STGPOOL**. (Чтобы предотвратить автоматический перенос на основе порога переноса, задайте значение 100 для параметра **HIGHMIG** и значение 0 для параметра **LOWMIG**, когда будете вводить команду **DEFINE STGPOOL**.)

- f. Нужно ли задавать задержку переноса?

Предпочтительный метод - задать ежедневный перенос с диска на ленту и не задавать задержку переноса, для которой требуется дополнительное планирование. Дополнительные сведения о задержках перенастройки смотрите в разделе [Перенос файлов в иерархии пулов хранения](#).

- g. Как можно вычислить число лентопротяжных устройств?

- 1) Определите собственную скорость перемещения данных накопителем, ознакомившись с документацией производителя. Чтобы получить оценку поддерживаемой скорости передачи данных в среде хранения, вычтите 30% из собственной скорости передачи данных.
- 2) Вычислите нужную скорость поглощения данных сервером. Затем разделите значение на поддерживаемую скорость передачи данных одним ленточным устройством. Результат будет указывать минимальное число накопителей для поддержки поглощения данных.
- 3) Вычислите число точек монтирования, которые требуются клиентам, создающим резервные копии данных на ленте, включая те клиенты, которые используют несколько сеансов. Точки монтирования можно распределить по окну резервного копирования, учитывая, что клиенты, вероятно, производят резервное копирование больших объектов, которые могут использовать большую часть этого окна.
- 4) Вычислите требования к производительности и число точек монтирования, которые требуются для выполнения задач по обслуживанию, например, переноса данных с диска на ленту и создания копий с ленты на ленту. Производя резервное копирование данных на ленту, можно избежать обработки переноса, но создание копий с ленты на ленту вдвое увеличит требования к ленточным накопителям.
- 5) Вычислите число дополнительных накопителей, которые могут потребоваться, например:

- Если ленточный накопитель работает неправильно, эта проблема повлияет на число доступных точек монтирования и скорость поглощения данных. Рассмотрите возможность предоставления запасных свободных накопителей. Например, если вам нужно пять ленточных накопителей для обычной работы, рассмотрите возможность предоставить два свободных накопителя.
- Для операций восстановления и получения могут потребоваться дополнительные ленточные накопители, если вы собираетесь одновременно запускать операции по поглощению данных и обслуживанию. Если потребуется, предоставьте дополнительные ленточные накопители и убедитесь, что они не используются, когда вы запускаете операции восстановления или получения.

h. Какие альтернативы существуют для оптимизации операций восстановления?

Можно использовать совместное размещение, чтобы повысить производительность системы и оптимизировать организацию данных. При совместном размещении можно сократить число томов, к которым придется обращаться при восстановлении больших объемов данных:

- В случае пулов хранения на основе дисков предпочтительный метод - это использование совместного размещения по узлам. Сервер размещает данные узла на как можно меньшем числе томов.
- В случае пулов хранения на основе лент предпочтительный метод - это использование совместного размещения по группам. При совместном размещении по группам сокращается неиспользуемое ленточное пространство, что позволяет совместно разместить на отдельных лентах больше данных.

Дополнительную информацию о совместном размещении смотрите в разделе [“Оптимизация операций путем включения совместного размещения файлов клиентов”](#) на стр. 177.

Если вы - опытный системный администратор, вы можете запланировать дополнительные действия для оптимизации операций восстановления. См. разделы [Оптимизация операций восстановления для клиентов](#), [Технологии резервного копирования файлов](#) и [MOVE NODEDATA \(перемещение данных узла в пуле хранения с последовательным доступом\)](#).

Хранение данных вне площадки

Чтобы упростить восстановление данных и как часть стратегии аварийного восстановления храните копии лент вне площадки.

Используйте функцию disaster recovery manager (DRM), чтобы сконфигурировать и автоматически сгенерировать план аварийного восстановления, содержащий информацию, сценарии и процедуры, необходимые для автоматического восстановления сервера и возврата данных клиентов после аварии. Выберите одну следующих возможностей хранения данных вне площадки как стратегию аварийного восстановления для защиты копий лент:

Сохранение вне площадки с одной производственной площадки

Тома хранения, например, ленточные картриджи и тома носителей, хранятся в расположении вне площадки. Курьер перевозит данные с места хранения вне площадки на площадку восстановления. Если произойдет авария, тома будут отправлены обратно на производственную площадку после восстановления оборудования и сервера IBM Spectrum Protect.

Сохранение вне площадки с площадкой восстановления

Курьер перевозит тома хранения с производственной площадки туда, где осуществляются хранение вне площадки. При наличии специальной площадки для восстановления можно сократить время восстановления по сравнению с одной производственной площадкой. Однако при таком способе повышается стоимость восстановления после аварий, так как нужно обслуживать больше аппаратных и программных средств. Например, площадка восстановления должен включать в себя совместимые ленточные устройства и программное обеспечение сервера IBM Spectrum Protect. Для возможности восстановления производственной площадки уже должен быть сконфигурирована и запущена площадка восстановления.

Электронное хранилище

Чтобы использовать электронное хранилище в качестве стратегии аварийного восстановления, на площадке восстановления должен быть работающий сервер IBM Spectrum Protect. Критические данные с производственной площадки сохраняются на площадке восстановления электронным способом. DRM также используется для хранения некритических данных вне площадки. При электронном сохранении критические данные перемещаются с площадки быстрее и чаще, чем при традиционных способах с использованием курьеров. Время восстановления сокращается, поскольку критические данные уже хранятся на площадке восстановления. Однако, поскольку площадка восстановления работает постоянно, стоимость стратегии аварийного восстановления выше, чем хранение вне площадки.

Понятия, связанные с данным

Подготовка к аварии и восстановление после аварии с использованием DRM

В IBM Spectrum Protect есть функция disaster recovery manager (DRM) для восстановления данных сервера и клиента при аварии.

Планирование защиты

Спланируйте защиту систем в решении IBM Spectrum Protect, используя управление доступом и аутентификацией, и рассмотрите возможность шифрования данных и передачи паролей.

Планирование ролей администратора

Задайте уровень полномочий, которые вы хотите назначить для решения IBM Spectrum Protect.

Администраторам можно назначить один из следующих уровней полномочий:

Система

У администраторов с системными полномочиями - высший уровень полномочий.

Администраторы с этим уровнем полномочий могут выполнить любую задачу. Они могут управлять всеми доменами политики и пулами хранения и предоставлять полномочия другим администраторам.

Политика

Администраторы, у которых есть полномочия политики, могут управлять всеми задачами, связанными с управлением политикой. Эти полномочия могут быть неограниченными или могут быть ограничены определенными доменами политики.

Хранение

Администраторы, у которых есть полномочия хранения, могут выделить ресурсы хранения для сервера и управлять ими.

Оператор

Администраторы, у которых есть полномочия оператора, могут управлять непосредственной работой сервера и доступностью таких носителей хранения, как ленточные библиотеки и накопители.

В сценариях в [Таблица 8 на стр. 27](#) представлены примеры того, почему вам может потребоваться назначить разные уровни полномочий, чтобы администраторы могли выполнять задачи:

Таблица 8. Сценарии для ролей администраторов	
Сценарий	Тип ID администратора, который нужно задать
Администратор в небольшой компании управляет сервером и отвечает за все операции сервера.	<ul style="list-style-type: none">Системные полномочия: 1 ID администратора

Таблица 8. Сценарии для ролей администраторов (продолжение)	
Сценарий	Тип ID администратора, который нужно задать
Администратор нескольких серверов также управляет всей системой. Несколько других администраторов управляют своими собственными пулами хранения.	<ul style="list-style-type: none"> Системные полномочия на всех серверах: 1 ID администратора для всех задач по администрированию системы Полномочия на хранение для назначенных пулов хранения: 1 ID администратора для каждого из других администраторов
Администратор управляет двумя серверами. Другой сотрудник помогает выполнять задачи по администрированию. Два помощника отвечают за то, чтобы производилось резервное копирование важных систем. Каждый помощник отвечает за мониторинг запланированных операций по резервному копированию на одном из серверов IBM Spectrum Protect.	<ul style="list-style-type: none"> Системные полномочия на обоих серверах: 2 ID администратора Полномочия оператора: 2 ID администраторов для помощников с доступом к серверу, за который отвечает каждый сотрудник

Задачи, связанные с данной

Управление администраторами

Администратор с системными полномочиями может выполнить любую задачу с сервером IBM Spectrum Protect, включая назначение уровней полномочий для других администраторов. Чтобы выполнить ряд задач, вам должны быть предоставлены полномочия путем назначения одного или нескольких уровней полномочий.

Планирование защищенной связи

План защиты взаимодействий между компонентами решения IBM Spectrum Protect.

Определите уровень защиты, требующийся для ваших данных, на основе нормативов и бизнес-требований, которые действуют в вашей компании.

Если для вашего бизнеса требуется высокий уровень защиты паролей и передаваемых данных, запланируйте реализацию защищенной связи на основе протоколов Transport Layer Security (TLS) или Secure Sockets Layer (SSL).

TLS и SSL обеспечивают защищенную связь между сервером и клиентом, но могут отрицательно влиять на производительность системы. Чтобы повысить производительность системы, используйте TLS для аутентификации без шифрования данных объектов. Чтобы указать, использует ли сервер TLS 1.2 для всего сеанса или только для аутентификации, смотрите описание опции клиента SSL для взаимодействий клиента с сервером и параметра **UPDATE SERVER=SSL** для взаимодействий сервера с сервером. Начиная с версии 8.1.2, TLS используется для аутентификации по умолчанию. Если вы решите использовать TLS для шифрования всего сеанса, используйте этот протокол только для сеансов, в которых это необходимо, и добавьте на сервер процессорные ресурсы, чтобы справиться с увеличением сетевого трафика. Также можно попробовать использовать другие опции. Например, в некоторых сетевых устройствах, например, в маршрутизаторах и коммутаторах, есть функция TLS или SSL.

TLS и SSL можно использовать для защиты некоторых или всех различных возможных путей связи, например:

- Центр операций: браузер с хабом; хаб с подчиненным сервером
- Клиент с сервером
- Сервер с сервером: репликация узлов

Задачи, связанные с данной

[Конфигурирование защищенной связи с использованием Transport Layer Security \(TLS\)](#)

Чтобы шифровать данные и защищать связь в вашей среде, на сервере и на клиенте резервного копирования и архивирования IBM Spectrum Protect включен протокол Secure Sockets Layer (SSL) или Transport Layer Security (TLS). Сертификат SSL используется для проверки требований связи между сервером и клиентом.

Планирование хранения зашифрованных данных

Определите, требуется ли вашей компании шифровать сохраняемые данные, и выберите способ, который лучше всего подходит для ваших требований.

Таблица 9. Выбор метода шифрования данных		
Бизнес-требование	Метод шифрования	Дополнительная информация
Защитите данные на уровне клиентуровень клиента.	Шифрование клиента IBM Spectrum Protect	Данные можно шифровать на уровне файлов, используя список include/exclude. Это позволяет обеспечить высокую степень контроля над тем, какие данные шифруются. На клиенте потребуются дополнительные вычислительные ресурсы, что может повлиять на производительность процессов резервного копирования и восстановления. Дополнительную информацию об этом методе смотрите в разделе Шифрование клиента IBM Spectrum Protect .
Защитите данные в томах пула хранения на ленточном накопителе.	На уровне программы	При использовании метода Приложение IBM Spectrum Protect управляет ключами шифрования для защиты данных в томах пула хранения. Вы должны особо тщательно подходить к защите резервных копий базы данных, так как ключи шифрования хранятся в базе данных сервера. Без доступа к резервным копиям базы данных и без сопоставления ключей шифрования данные восстановить невозможно. Использовать этот метод для шифрования резервных копий базы данных, экспортируемых данных или наборов резервных копий нельзя. Дополнительную информацию о методе Приложение смотрите в разделе “Методы шифрования лент” на стр. 127.
Защитите данные на ленточном накопителе.	На уровне библиотеки	При использовании метода Библиотека библиотека управляет ключами шифрования. Можно шифровать как данные в пулах хранения, так и другие данные на ленточном накопителе. Вы можете управлять тем, какие тома будут зашифрованы, используя их штрих-коды с серийными номерами. Дополнительную информацию о методе Библиотека смотрите в разделе “Методы шифрования лент” на стр. 127.
Защитите данные на ленточном накопителе.	На уровне системы	При использовании метода Система шифрованием управляет драйвер устройств или операционная система AIX. Этот метод шифрования доступен только в операционной системе AIX. Можно шифровать как данные в пулах хранения, так и другие данные на ленточном накопителе. Дополнительную информацию о методе Система смотрите в разделе “Методы шифрования лент” на стр. 127.

Планирование доступа через брандмауэр

Определите, какие у вас заданы брандмауэры и какие порты должны быть открыты, чтобы решение IBM Spectrum Protect работало.

В разделе Таблица 10 на стр. 30 описаны порты, используемые сервером, клиентом и компонентом Центр операций.

Таблица 10. Порты, используемые сервером, клиентом и компонентом Центр операций			
Элемент	По умолчанию	Направление	Описание
Базовый порт (TCP PORT)	1500	Исходящие/входящие	Для каждого экземпляра сервера требуется уникальный порт. Можно задать альтернативный номер порта. Опция TCPPORT принимает от клиента как сеансы TCP/IP, так и сеансы с поддержкой SSL. Чтобы задать значения портов для трафика клиента администрирования, можно использовать опцию TCPADMINPORT и опцию ADMINONCLIENTPORT .
SSL-only port (SSLTCP PORT)	Значения по умолчанию нет	Исходящие/входящие	Этот порт используется, если вы хотите ограничить взаимодействия на порту только сеансами, поддерживающими SSL. Сервер может поддерживать взаимодействия как SSL, так и не SSL, используя опции TCPPORT или TCPADMINPORT .
SMB	45	Входящие/исходящие	Этот порт используется мастерами конфигурирования, которые, используя собственные протоколы, взаимодействуют с несколькими хостами.
SSH	22	Входящие/исходящие	Этот порт используется мастерами конфигурирования, которые, используя собственные протоколы, взаимодействуют с несколькими хостами.
SMTP	25	Исходящие	Этот порт используется для отправки оповещений с сервера по электронной почте.
Репликация	Значения по умолчанию нет	Исходящие/входящие	Порт и протокол для исходящего порта при репликации заданы командой DEFINE SERVER , которая используется, чтобы настроить репликацию. Входящие порты для репликации - это порты TCP и порты SSL, заданные для исходного сервера в команде DEFINE SERVER .
Порт клиентских расписаний	Порт клиента: 1501	Исходящие	Клиент осуществляет прием на указанном порту и передает номер порта серверу. Сервер соединяется с клиентом, если используется планирование по приглашению сервера. Можно задать альтернативный номер порта в файле опций клиента.
Длительно выполн. сеансы	Параметр KEEPALIVE: YES	Исходящие	Если разрешена опция KEEPALIVE , то контрольные пакеты отправляются во время сеансов клиент-сервер, чтобы не дать программе брандмауэра закрыть длительно выполняющиеся, неактивные соединения.
Центр операций	HTTPS: 11090	Входящие	Эти порты используются для веб-браузера компонента Центр операций. Можно задать альтернативный номер порта.

Таблица 10. Порты, используемые сервером, клиентом и компонентом Центр операций
(продолжение)

Элемент	По умолчанию	Направление	Описание
Порт службы управления клиентами	Порт клиента: 9028	Входящие	Если вы собираетесь использовать компонент Служба управления клиентами IBM Spectrum Protect, порт службы управления клиентами должен быть доступен из компонента Центр операций. Убедитесь, что брандмауэры не запрещают соединения. Служба управления клиентами использует порт TCP сервера клиентского узла для аутентификации, используя административный сеанс.

Информация, связанная с данной

[Сбор диагностической информации с помощью служб управления клиентами IBM Spectrum Protect](#)
[опция сервера ADMINONCLIENTPORT](#)

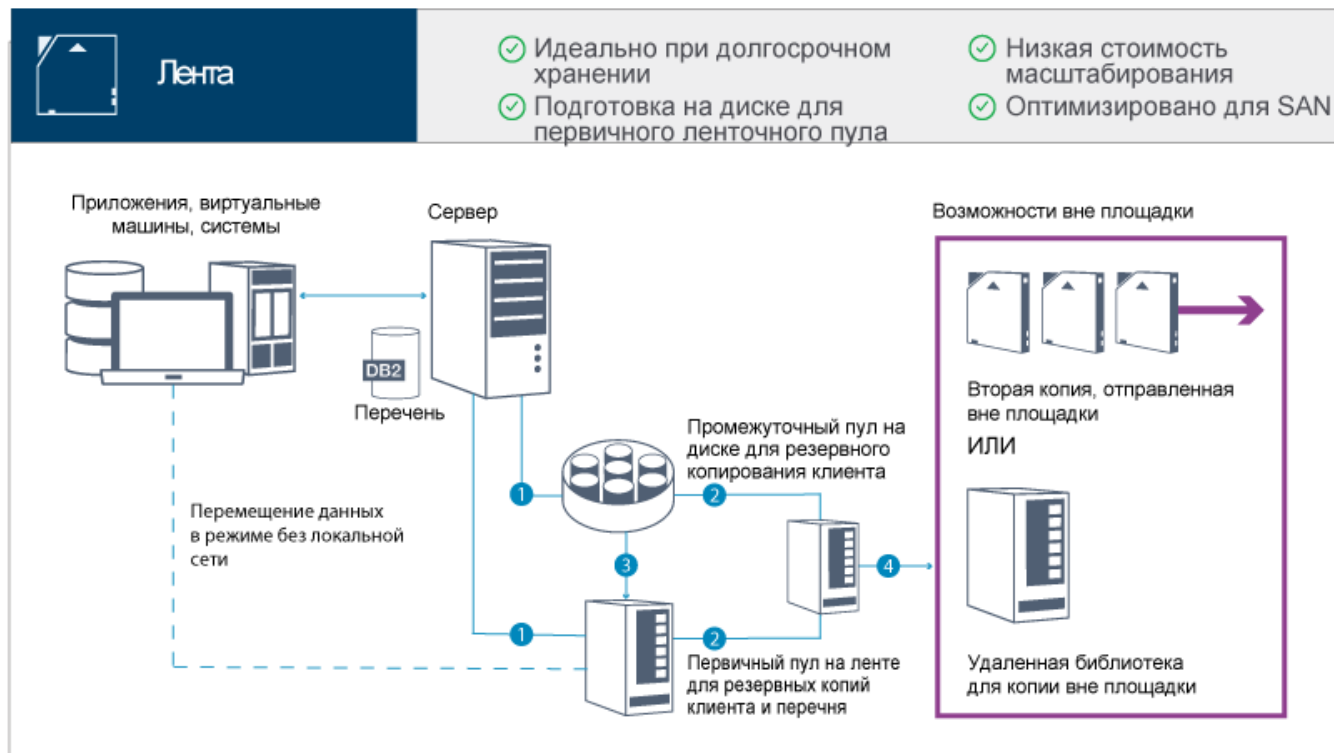
[DEFINE SERVER \(Задать сервер для обмена данными между серверами\)](#)

[Опция сервера TCPADMINPORT](#)

[опция сервера TCPPORT](#)

Часть 2. Реализация решения по защите данных на основе ленты

Решение на основе ленты использует резервное копирование с диска на диск и на ленту и применяет промежуточное сохранение на диске для оптимизации хранения. Реализуя решение на лентах, можно включить долгосрочное хранение данных и добиться экономичной масштабируемости.



Советы:

- В описанном решении данные *переносятся* из дисковых пулов хранения в ленточные пулы хранения. Однако вместо переноса данных можно использовать функцию tiering-to-tape (разбиение на слои на ленту), введенную в IBM Spectrum Protect версии 8.1.8. Используя эту функцию, можно автоматически разбивать данные на слои из пулов хранения каталогов-контейнеров на диске в ленточную систему хранения. Можно указать, что все данные будут разбиты на слои в соответствии с заданным порогом возраста или что только неактивные данные будут разбиты на слои в зависимости от порога возраста. Дополнительную информацию о том, как данные разбиваются на слои в ленточную систему хранения, смотрите в разделе [Разбиение данных на слои для облачного или ленточной системы хранения](#).
- Описанное решение не включает в себя репликацию узлов. Если вы хотите использовать репликацию узлов, чтобы создать резервную копию пула хранения с диска на диск, убедитесь, что операция репликации завершилась, прежде чем переносить данные с диска на ленту. Репликацию узлов также можно использовать для резервного копирования пула хранения на локальном ленточном устройстве в пул хранения копий на локальном ленточном устройстве.

Путеводитель по реализации

Для настройки решения на основе ленты нужно сделать следующее:

- [Настройте систему](#)
- [Установите сервер и Центр операций.](#)

3. [Сконфигурируйте сервер и Центр операций.](#)
4. [Подключите ленточные устройства для сервера.](#)
5. [Сконфигурируйте ленточные библиотеки для использования сервером.](#)
6. [Настройте иерархию пула хранения.](#)
7. [Установите и сконфигурируйте клиенты.](#)
8. [Сконфигурируйте перемещение данных в режиме без локальной сети.](#)
9. [Выберите метод шифрования и сконфигурируйте шифрование.](#)
10. [Настройте операции ленточной системы хранения.](#)
11. [Завершите реализацию.](#)

Настройка системы

Чтобы настроить систему, нужно сначала сконфигурировать дисковое оборудование хранения и серверную систему для IBM Spectrum Protect.

Об этой задаче

Совет: Здесь описаны процедуры настройки сервера и дисковой системы хранения. Чтобы приступить к настройке ленточных устройств, смотрите раздел [“Подключение ленточных устройств к серверу”](#) на стр. 78.

Конфигурирование оборудования систем хранения

Чтобы оптимизировать дисковое хранение, прочтите рекомендации по настройке дискового пространства хранения с помощью IBM Spectrum Protect. Затем задайте соединение между сервером и дисковыми устройствами хранения и выполните остальные задачи по конфигурированию.

Прежде чем начать

Рекомендации по настройке дискового пространства хранения смотрите в разделе [Контрольный список для пулов хранения на устройствах DISK или FILE](#)

Процедура

1. Задайте соединение между сервером и устройствами хранения, следуя приведенным ниже рекомендациям:
 - Используйте коммутируемое или прямое усоединение для соединений Fibre Channel.
 - Подберите число портов для соединения и учетную запись для необходимой ширины полосы пропускания.
 - Подберите число портов для соединения на сервере и число портов хоста в дисковой системе.
2. Убедитесь, что драйверы устройств и встроенная микропрограмма в системе сервера, адаптеров и операционной системы, являются современными и находятся на рекомендуемых уровнях.
3. Сконфигурируйте массивы хранения. Убедитесь, что вы правильно произвели планирование, чтобы обеспечить оптимальную производительность.
Дополнительную информацию смотрите в разделе [“Планирование дисковой системы хранения”](#) на стр. 14.
4. Убедитесь, что у системы сервера есть доступ к созданным дисковым томам. Сделайте следующее:
 - а) Если система подключена к коммутатору Fibre Channel, произведите зонирование сервера, чтобы увидеть диски.

- b) Отобразите все тома, чтобы сообщить дисковой системе, что данному серверу разрешено видеть каждый диск.
5. Убедитесь, что ленточные и дисковые устройства используют разные порты адаптера шины хоста (Host Bus Adapter, HBA). Управляйте вводом-выводом на ленты и диски с использованием SAN. Используйте отдельные порты Fibre Channel для ввода-вывода на магнитную ленту и на диск.

Задачи, связанные с данной

Конфигурирование ввода-вывода с несколькими путями

Можно разрешить и сконфигурировать поддержку нескольких путей для дисковой системы хранения. Подробные инструкции смотрите в документации, прилагаемой к вашим аппаратным средствам.

Установка операционной системы сервера

Установите операционную систему на компьютере сервера и убедитесь, что выполнены требования сервера IBM Spectrum Protect. Скорректируйте параметры операционной системы, как указано.

Установка в системах AIX

Выполните следующие действия, чтобы установить AIX в системе сервера.

Procedure

1. Установите AIX версии 7.1 TL4, SP6 или новее в соответствии с инструкциями производителя.
2. Сконфигурируйте параметры TCP/IP согласно инструкциям по установке операционной системы.
3. Откройте файл `/etc/hosts` и сделайте следующее:

- Обновите файл, включив в него IP-адрес и имя хоста для сервера. Например:

```
192.0.2.7 server.yourdomain.com server
```

- Убедитесь, что файл содержит запись для localhost с адресом 127.0.0.1. Например:

```
127.0.0.1 localhost
```

4. Включите полты выполнения ввода-вывода AIX, введя следующую команду:

```
chdev -l iocp0 -P
```

На производительность сервера может влиять определение часового пояса по Олсону (Olson).

5. Чтобы оптимизировать производительность, измените формат часового пояса с Olson на POSIX. Чтобы обновить параметр часового пояса, используйте следующий формат команды:

```
chtz=локальный_часовой_пояс, дата/время, дата/время
```

Например, если вы находитесь в Тьюсоне (Аризона), где используется стандартное горное время, то вы бы, чтобы перейти к формату POSIX, ввели бы следующую команду:

```
chtz MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00
```

6. В файле `.profile` пользователя экземпляра, убедитесь, что установлены следующие переменные среды:

```
export MALLOCOPTIONS=multiheap:16
```

В более поздних версиях сервера IBM Spectrum Protect это значение задается автоматически при запуске сервера. Если пользователь экземпляра недоступен, то выполните этот шаг позже, когда пользователь экземпляра станет доступен.

7. Настройте систему на создание полных файлов ядра приложения. Введите следующую команду:

```
chdev -l sys0 -a fullcore=true -P
```

8. Чтобы обеспечить взаимодействия с сервером и компонентом Центр операций, убедитесь, что на всех брандмауэрах, которые могут существовать, открыты следующие порты:

- Для связи с сервером откройте порт 1500.
- Чтобы обеспечить защищенную связь с компонентом Центр операций, откройте порт 11090 на хаб-сервере.

Если вы не используете значения портов по умолчанию, то убедитесь, что используемые вами порты открыты.

9. Включите усовершенствования высокой производительности TCP. Введите следующую команду:

```
no -p -o rfc1323=1
```

10. Чтобы обеспечить оптимальную пропускную способность и надежность, свяжите вместе два порта 10 Gb Ethernet в случае средней системы и четыре порта 10 Gb Ethernet в случае крупной системы. Используйте инструмент System Management Interface Tool (SMIT), чтобы связать порты друг с другом, используя Etherchannel.

При тестировании использовались следующие параметры:

режим	8023ad	
auto_recovery	yes	Включить автоматическое восстановление после передачи управления
backup_adapter	NONE	Адаптер, используемый при ошибке всего канала
hash_mode	src_dst_port	Указывает, как выбирается исходящий адаптер
interval	long	Определяет значение интервала для режима IEEE 802.3ad
mode	8023ad	Режим EtherChannel для операции
netaddr	0	Адрес для команды ping
no_loss_failover	yes	Включает передачу управления без потери данных после неудачного завершения ping
num_retries	3	Сколько раз повторять ping, прежде чем заключить о неудаче
retry_time	1	Время ожидания (в сек.) между командами ping
use_alt_addr	no	Включить другой адрес EtherChannel
use_jumbo_frame	no	Включить фреймы Gigabit Ethernet Jumbo

11. Убедитесь, что предельные значения для ресурсов процессов пользователя, которые также называются *ulimit*, заданы согласно рекомендациям в разделе [Table 11 on page 36](#). Если значения *ulimit* заданы неправильно, вы можете столкнуться с нестабильностью сервера или ошибкой ответа сервера.

Table 11. Предельные значения для пользователей (ulimit)			
Тип пользовательского предела	Установка	Значение	Команда для запроса значения
Максимальный размер создаваемых файлов ядра	core	Без ограничений	ulimit -Hc
Максимальный размер сегмента данных для процесса	данные	Без ограничений	ulimit -Hd
Максимальный размер файлов	fsize	Без ограничений	ulimit -Hf

Table 11. Предельные значения для пользователей (ulimit) (continued)			
Тип пользовательского предела	Установка	Значение	Команда для запроса значения
Максимальное число открытых файлов	nofile	65536	ulimit -Hn
Максимальное время процессора в секундах	cpu	Без ограничений	ulimit -Ht
Максимальное число процессов пользователей	nproc	16384	ulimit -Hu

Если вам нужно изменить какие-либо предельные значения для пользователей, следуйте инструкциям в документации для вашей операционной системы.

Установка в системах Linux

Выполните следующие действия, чтобы установить Linux x86_64 в системе сервера.

Before you begin

Операционная система устанавливается на внутренних жестких дисках. Сконфигурируйте внутренние жесткие диски, используя аппаратный массив RAID 1. Например, если вы конфигурируете небольшую систему, два внутренних диска по 300 ГБ зеркально отражаются в RAID 1, в результате чего для программы установки операционной системы будет доступен один диск в 300 ГБ.

Procedure

1. Установите Red Hat Enterprise Linux версии 7.4 или новее в соответствии с инструкциями производителя.

Получите загрузочный DVD-диск, содержащий Red Hat Enterprise Linux версии 7.4 и запустите свою систему с этого DVD-диска. Опции установки смотрите в приведенных ниже рекомендациях. Если элемент не упомянут в приведенном ниже списке, оставьте для него значение по умолчанию.

- a) После запуска DVD-диска выберите в меню **Установить или обновить существующую систему**.
- b) В окне с приветствием выберите **Проверить этот носитель и установить Red Hat Enterprise Linux 7.4**.
- c) Выберите предпочтения языка и клавиатуры.
- d) Выберите свое расположение, чтобы задать нужный часовой пояс.
- e) Выберите **Выбор программ**, а затем в следующем окне выберите **Сервер с графическим пользовательским интерфейсом**.
- f) На странице сводной информации установки щелкните по **Пункт назначения установки** и проверьте следующее:
 - В качестве пункта назначения установки выбирается локальный диск на 300 ГБ.
 - В разделе Другие опции хранения выбирается опция Автоматически сконфигурировать разбиение на разделы.

Щелкните по **Готово**.

- g) Щелкните по **Начать установку**.

После запуска установки задайте пароль пользователя root для учетной записи пользователя root.

По завершении установки перезапустите систему и войдите в систему от имени пользователя root. Введите команду **df**, чтобы проверить базовое разбиение на разделы.

Например, в тест-системе первоначальные разделы выдали следующий результат:

```
[root@tvapp02]# df -h
Файловая сист.      50G   3.0G   48G   6% /
/dev/mapper/rhel-root
devtmpfs             32G    0    32G   0% /dev
tmpfs                32G   92K   32G   1%  /dev/shm
tmpfs                32G   8.8M   32G   1%  /run
tmpfs                32G    0    32G   0%  /sys/fs/cgroup
/dev/mapper/rhel-home 220G   37M   220G   1% /home
/dev/sda1             497M  124M   373M  25% /boot
```

2. Сконфигурируйте параметры TCP/IP согласно инструкциям по установке операционной системы.

Чтобы обеспечить оптимальную пропускную способность и надежность, рассмотрите возможность связать вместе несколько сетевых портов. Свяжите вместе два порта для системы среднего размера или четыре порта для крупной системы. Это можно выполнить, создав сетевое соединение Link Aggregation Control Protocol (LACP), которое агрегирует несколько подчиненных портов в одно логическое соединение. Предпочтительный метод состоит в том, чтобы использовать режим связи 802.3ad, параметр **miimon**, равный 100, и параметр **xmit_hash_policy**, равный layer3+4.

Restriction: Для использования сетевого соединения LACP у вас должен быть сетевой коммутатор, поддерживающий LACP.

Дополнительные инструкции по конфигурированию привязанных сетевых соединения при использовании Red Hat Enterprise Linux версии 7 смотрите в документе: [Создать интерфейс привязки каналов](#).

3. Откройте файл /etc/hosts и сделайте следующее:

- Обновите файл, включив в него IP-адрес и имя хоста для сервера. Например:

```
192.0.2.7 server.yourdomain.com server
```

- Убедитесь, что файл содержит запись для localhost с адресом 127.0.0.1. Например:

```
127.0.0.1 localhost
```

4. Установите компоненты, необходимые для установки сервера. Выполните описанные ниже шаги, чтобы создать репозиторий Yellowdog Updater Modified (YUM) и установить необходимые пакеты.

- a) Смонтируйте DVD-диск установки Red Hat Enterprise Linux в системном каталоге. Например, чтобы смонтировать его в каталоге /mnt, введите следующую команду:

```
mount -t iso9660 -o ro /dev/cdrom /mnt
```

- b) Убедитесь, что DVD-диск смонтирован, введя команду **mount**.

Должна появиться выходная информация, аналогичная следующему примеру:

```
/dev/sr0 on /mnt type iso9660
```

- c) Перейдите в каталог репозитория YUM, введя следующую команду:

```
cd /etc/yum/repos.d
```

Если каталог `repos.d` не существует, создайте его.

- d) Вызовите список содержимого каталога:


```
ls rhel-source.repo
```

- е) Переименуйте исходный файл геро, введя команду **mv**.
Например:

```
mv rhel-source.repo rhel-source.repo.orig
```

- ф) Создайте новый файл геро, используя текстовый редактор.
Например, чтобы использовать редактор **vi**, введите следующую команду:

```
vi rhel74_dvd.repo
```

- г) Добавьте в новый файл геро следующие строки. Параметр **baseurl** задает точку монтирования каталога:

```
[rhel74_dvd]
name=DVD Redhat Enterprise Linux 7.4
baseurl=file:///mnt
enabled=1
gpgcheck=0
```

- h) Установите необходимый пакет **ksh.x86_64**, введя команду **yum**.
Например:

```
yum install ksh.x86_64
```

5. По завершении установки программы вы сможете восстановить исходные значения репозитория YUM, выполнив следующие шаги:

- а) Размонтируйте DVD-диск установки Red Hat Enterprise Linux, введя следующую команду:

```
umount /mnt
```

- б) Перейдите в каталог репозитория YUM, введя следующую команду:

```
cd /etc/yum/repos.d
```

- с) Переименуйте созданный вами файл геро:

```
mv rhel74_dvd.repo rhel74_dvd.repo.orig
```

- д) Переименуйте исходный файл, используя его исходное имя:

```
mv rhel-source.repo.orig rhel-source.repo
```

6. Определите, требуется ли измерения параметров ядра. Сделайте следующее:

- а) Используйте команду **sysctl -a**, чтобы вывести список значений параметров.
б) Проанализируйте результаты, следуя рекомендациям в разделе [Table 12 on page 39](#), чтобы определить, не требуются ли какие-либо изменения.
с) Если требуются изменения, задайте параметры в файле **/etc/sysctl.conf**.
Изменения файлов применяются при запуске системы.

Tip: Автоматически корректируйте значения параметров ядра и устраните необходимость обновления этих параметров вручную. В Linux продукт программного обеспечения баз данных Db2 автоматически корректирует значения параметров ядра взаимодействий между процессами (interprocess communication, IPC) до предпочтительных значений. Чтобы получить дополнительную информацию о значениях параметров ядра, ищите параметры ядра Linux в публикации [Документация к IBM Db2 версии 11.5](#).

Table 12. Оптимальные значения параметра ядра Linux	
Параметр	Описание
kernel.shmmni	Максимальное число сегментов.

Table 12. Оптимальные значения параметра ядра Linux (continued)	
Параметр	Описание
kernel.shmmax	Максимальный размер сегмента совместно используемой памяти (в байтах). Этот параметр нужно задать до автоматического запуска сервера IBM Spectrum Protect при запуске системы.
kernel.shmall	Максимальное число размещенных страниц совместно используемой памяти.
kernel.sem Существует четыре значения для параметра kernel.sem .	(SEMMSL) Максимальное число семафоров на массив.
	(SEMMNS) Максимальное число семафоров на систему.
	(SEMOPM) Максимальное число операций на вызов семафора.
	(SEMMNI) Максимальное число массивов.
kernel.msgmni	Максимальное число очередей сообщений уровня системы.
kernel.msgmax	Максимальный размер сообщения (в байтах).
kernel.msgmnb	Максимальный размер очереди по умолчанию (в байтах).
kernel.randomize_va_space	Параметр kernel.randomize_va_space конфигурирует использование памяти ASLR для ядра. Разрешает ASLR для серверов V7.1 и новее. Дополнительные подробности об ASLR Linux и Db2 смотрите в документе техническое замечание 1365583 .
vm.swappiness	Параметр vm.swappiness определяет, может ли ядро выполнять свопинг для памяти программы из физической оперативной памяти. Дополнительную информацию о параметрах ядра смотрите по адресу Информация о Db2 .
vm.overcommit_memory	Параметр vm.overcommit_memory влияет на то, какой объем виртуальной памяти ядро разрешает выделить. Дополнительную информацию о параметрах ядра смотрите по адресу Информация о Db2 .

7. Откройте порты брандмауэра для взаимодействия с сервером. Сделайте следующее:

- Определите зону, используемую сетевым интерфейсом. По умолчанию, это общедоступная зона.

Введите следующую команду:

```
# firewall-cmd --get-active-zones
public
interfaces: ens4f0
```

- Чтобы использовать адрес порта по умолчанию для взаимодействия с сервером, откройте порт TCP/IP 1500 на брандмауэре Linux.

Введите следующую команду:

```
firewall-cmd --zone=public --add-port=1500/tcp --permanent
```

Если вы хотите использовать какое-либо значение, отличающееся от значения по умолчанию, вы можете задать число в диапазоне 1024-32767. Если вы откроете порт, отличающийся от порта по умолчанию, вы должны будете указать порт при запуске сценария конфигурирования.

- с) Если вы собираетесь использовать эту систему как хаб, откройте порт 11090, который является портом по умолчанию для защищенных взаимодействий (https).

Введите следующую команду:

```
firewall-cmd --zone=public --add-port=11090/tcp --permanent
```

- d) Чтобы изменения вступили в силу, заново загрузите определения брандмауэра.

Введите следующую команду:

```
firewall-cmd --reload
```

8. Убедитесь, что предельные значения для ресурсов процессов пользователя, которые также называются *ulimit*, заданы согласно рекомендациям в разделе [Table 13 on page 41](#). Если значения *ulimit* заданы неправильно, вы можете столкнуться с нестабильностью сервера или ошибкой ответа сервера.

Table 13. Предельные значения для пользователей (<i>ulimit</i>)			
Тип пользовательского предела	Установка	Значение	Команда для запроса значения
Максимальный размер создаваемых файлов ядра	core	Без ограничений	<code>ulimit -Hc</code>
Максимальный размер сегмента данных для процесса	данные	Без ограничений	<code>ulimit -Hd</code>
Максимальный размер файлов	fsize	Без ограничений	<code>ulimit -Hf</code>
Максимальное число открытых файлов	nofile	65536	<code>ulimit -Hn</code>
Максимальное время процессора в секундах	cpu	Без ограничений	<code>ulimit -Ht</code>
Максимальное число процессов пользователей	nproc	16384	<code>ulimit -Hu</code>

Если вам нужно изменить какие-либо предельные значения для пользователей, следуйте инструкциям в документации для вашей операционной системы.

Установка в системах Windows

Установите Microsoft Windows Server 2012 Standard Edition на компьютере-сервере и подготовьте систему к установке и конфигурированию сервера IBM Spectrum Protect.

Procedure

1. Установите Windows Server 2016 Standard Edition, согласно инструкциям изготовителя.
2. Измените политики управления учетными записями Windows, выполнив следующие шаги:
 - а) Откройте редактор локальной политики защиты, выполнив `secpol.msc`.
 - б) Выберите **Локальные политики > Опции защиты** и убедитесь, что отключены следующие политики управления учетными записями пользователей:
 - Режим Утверждать администраторов для встроенной учетной записи Администратор
 - Запускать всех администраторов в режиме Утверждать администраторов
3. Сконфигурируйте параметры TCP/IP согласно инструкциям по установке операционной системы.
4. Примените обновления Windows и включите дополнительные функции, выполнив следующие шаги:
 - а) Примените последние обновления Windows Server 2016.
 - б) Установите и включите функцию Windows 2012 R2 Microsoft .NET Framework 3.5 при помощи менеджера сервера Windows.
 - в) Если потребуется, обновите драйверы устройств FC и Ethernet HBA до новых уровней.
 - г) Установите драйвер ввода-вывода с несколькими путями, соответствующий используемой вами дисковой системе.
5. Откройте порт TCP/IP по умолчанию, 1500, для связи с сервером IBM Spectrum Protect. Например, введите следующую команду:

```
netsh advfirewall firewall add rule name="Backup server port 1500"
dir=in action=allow protocol=TCP localport=1500
```

6. На хаб-сервере Центра операций откройте порт по умолчанию для защищенной (https) связи с компонентом Центр операций.
Номер порта - 11090.
Например, введите следующую команду:

```
netsh advfirewall firewall add rule name="Центр операций port 11090"
dir=in action=allow protocol=TCP localport=11090
```

Конфигурирование ввода-вывода с несколькими путями

Можно разрешить и сконфигурировать поддержку нескольких путей для дисковой системы хранения. Подробные инструкции смотрите в документации, прилагаемой к вашим аппаратным средствам.

Системы AIX

Выполните описанные ниже шаги, чтобы включить и сконфигурировать поддержку нескольких путей для дисковой системы хранения.

Процедура

1. Определите адрес порта Fibre Channel, который нужно использовать для определения хоста в дисковой подсистеме. Введите команду **lscfg** для каждого порта.
 - В небольших и средних системах введите следующие команды:

```
lscfg -vps -l fcs0 | grep "Network Address"
lscfg -vps -l fcs1 | grep "Network Address"
```

- В крупных системах введите следующие команды:

```
lscfg -vps -l fcs0 | grep "Network Address"
lscfg -vps -l fcs1 | grep "Network Address"
```

```
lscfg -vps -l fcs2 | grep "Network Address"
lscfg -vps -l fcs3 | grep "Network Address"
```

2. Убедитесь, что установлены следующие наборы файлов AIX:

- devices.common.IBM.mpio.rte
- devices.fcp.disk.rte

3. Введите команду **cfgmgr**, чтобы система AIX пересканировала оборудование и обнаружила доступные диски. Например:

```
cfgmgr
```

4. Чтобы вызвать список доступных дисков, введите следующую команду:

```
lsdev -Ccdisk
```

Выходная информация команды выглядит, как в следующем примере:

```
hdisk0  Доступно 00-00-00 SAS Дисковый накопитель
hdisk1  Доступно 00-00-00 SAS Дисковый накопитель
hdisk2  Доступно 01-00-00 SAS Дисковый накопитель
hdisk3  Доступно 01-00-00 SAS Дисковый накопитель
hdisk4  Доступно 06-01-02 MPIO IBM 2076 Диск FC
hdisk5  Доступно 07-01-02 MPIO IBM 2076 Диск FC
...
```

5. Используйте выходную информацию команды **lsdev**, чтобы найти и представить в виде списка ID устройств для каждого дискового устройства.

Например, ID устройства может быть hdisk4. Сохраните список ID устройств для использования при создании файловых систем для сервера IBM Spectrum Protect.

6. Скоррелируйте ID устройств SCSI с LUN отдельных дисков из дисковой системы, перечислив подробную информацию о всех физических томах в системе. Введите следующую команду:

```
lspv -u
```

В системе IBM Storwize примером того, что показано для каждого устройства, является следующая информация:

```
hdisk4 00f8cf083fd97327 Нет активен
3321360050763008101057800000000000003004214503IBMfcpr
```

В примере значение **60050763008101057800000000000030** - это UID тома, сообщенный интерфейсом управления Storwize.

Чтобы проверить размер дисков (в мегабайтах) и сравнить его с тем, что указано для системы, введите следующую команду:

```
bootinfo -s hdisk4
```

Системы Linux

Выполните описанные ниже шаги, чтобы включить и сконфигурировать поддержку нескольких путей для дисковой системы хранения.

Процедура

1. Внесите изменения в файл `/etc/multipath.conf`, чтобы включить поддержку нескольких путей для хостов Linux.

Если файл `multipath.conf` не существует, его можно создать, введя следующую команду:

```
mpathconf --enable
```

В файле `multipath.conf` при тестировании в системе хранения IBM FlashSystem были заданы следующие параметры:

```
defaults {
    user_friendly_names no
}

devices {
    device {
        vendor "IBM "
        product "2145"
        path_grouping_policy group_by_prio
        user_friendly_names no
        path_selector "round-robin 0"
        prio "alua"
        path_checker "tur"
        failback "immediate"
        no_path_retry 5
        rr_weight uniform
        rr_min_io_rq "1"
        dev_loss_tmo 120
    }
}
```

2. Задайте запуск поддержки нескольких путей при запуске системы.

Введите следующие команды:

```
systemctl enable multipathd.service
systemctl start multipathd.service
```

3. Чтобы убедиться, что диски видны операционной системе и управляются поддержкой нескольких путей, введите следующую команду:

```
multipath -l
```

4. Убедитесь, что перечислены все устройства и что число путей соответствует ожидаемому. Чтобы определить, какие диски указаны, можно использовать информацию о размере и ID устройств.

Например, в следующей выходной информации показано, что у диска на 2 ТБ есть две группы путей и четыре активных пути. Размер 2 ТБ подтверждает, что диск соответствует файловой системе пула. Используйте часть полного числового ID устройства (в данном примере, 12), чтобы найти том в интерфейсе управления дисковой системой.

```
[root@tapsrv01 code]# multipath -l
36005076802810c50980000000000012 dm-43 IBM,2145
size=2.0T features='1 queue_if_no_path' hwhandler='0' wp=rw
|+- policy='round-robin 0' prio=0 status=active
|  |- 2:0:1:18 sdcw 70:64 active undef running
|  `-- 4:0:0:18 sdgb 131:112 active undef running
`+- policy='round-robin 0' prio=0 status=enabled
|  |- 1:0:1:18 sdat 66:208 active undef running
|  `-- 3:0:0:18 sddy 128:0 active undef running
```

- а) Если потребуется, исправьте назначения хостов для LUN диска и произведите принудительное пересканирование шины.

Например:

```
echo "- - -" > /sys/class/scsi_host/host0/scan
echo "- - -" > /sys/class/scsi_host/host1/scan
echo "- - -" > /sys/class/scsi_host/host2/scan
```

Также можно перезапустить систему, чтобы пересканировать назначения хостов для LUN дисков.

- б) Убедитесь, что теперь диски доступны для ввода-вывода по нескольким путям, снова введя команду **multipath -l**.
5. Используйте выходную информацию команды `multipath`, чтобы найти и представить в виде списка ID устройств для каждого дискового устройства.

Например, ID устройства для вашего диска в 2 ТБ - это 36005076802810c509800000000000012.

Сохраните список ID устройств для использования в следующем шаге.

Системы Windows

Выполните описанные ниже шаги, чтобы включить и сконфигурировать поддержку нескольких путей для дисковой системы хранения.

Процедура

1. Убедитесь, что установлена функция ввода-вывода по нескольким путям. Если потребуется, установите дополнительные драйверы нескольких путей, связанные с поставщиками.
2. Чтобы убедиться, что диски видны операционной системе и управляются вводом-выводом по нескольким путям, введите следующую команду:

```
c:\program files\IBM\SDDDSM\datapath.exe query device
```

3. Ознакомьтесь с выходной информацией для поддержки нескольких путей и убедитесь, что перечислены все устройства и что число путей соответствует ожидаемому. Чтобы определить, какие диски указаны, можно использовать информацию о размере и серийных номерах устройств.

Например, используя часть полного серийного номера устройства (в данном примере, 34), вы сможете искать том в интерфейсе управления дисковой системой. Размер 2 ТБ подтверждает, что диск соответствует файловой системе пула хранения.

```
№ УСТР.    4  ИМЯ УСТРОЙСТВА: Disk5 Part0  ТИП: 2145  ПОЛИТИКА: ОПТИМИЗИРОВАННАЯ
СЕР.НОМ.: 60050763008101057800000000000034  РАЗМЕР LUN: 2.0 ТБ
```

№ пути	Адаптер/Жесткий диск	Состояние	Режим	Выбор	Ошибки
0	Scsi Port2 Bus0/Disk5 Part0	OPEN	NORMAL	0	0
1	Scsi Port2 Bus0/Disk5 Part0	OPEN	NORMAL	27176	0
2	Scsi Port3 Bus0/Disk5 Part0	OPEN	NORMAL	28494	0
3	Scsi Port3 Bus0/Disk5 Part0	OPEN	NORMAL	0	0

4. Создайте список ID дисковых устройств, используя серийные номера, возвращенные в выходной информации нескольких путей в предыдущем шаге.

Например, ID устройства для вашего диска в 2 ТБ - это 60050763008101057800000000000034

Сохраните список ID устройств для использования в следующем шаге.

5. Чтобы привести новые диски в подключенное состояние и снять атрибут "только для чтения", выполните `diskpart.exe` со следующими командами. Повторите для каждого из дисков:

```
diskpart
select Disk 1
online disk
attribute disk clear readonly
select Disk 2
online disk
attribute disk clear readonly
< ... >
select Disk 49
online disk
attribute disk clear readonly
exit
```

Создание ID пользователя для сервера

Создайте ID пользователя, который станет владельцем экземпляра сервера IBM Spectrum Protect. Вы укажете этот ID пользователя при создании экземпляра сервера при первоначальном конфигурировании сервера.

About this task

В ID пользователя можно использовать только буквы в нижнем регистре (a-z), цифры (0-9) и символ подчеркивания (_). ID пользователя и имя группы должны соответствовать следующим правилам:

- Длина не должна превышать 8 символов.
- ID пользователя не может начинаться с *ibm*, *sql*, *sys* или цифры.
- В качестве ID пользователя или имени группы нельзя использовать *user*, *admin*, *guest*, *public*, *local* или какое-либо зарезервированное слово SQL.

Procedure

1. Чтобы создать ID пользователя, используйте команды операционной системы.

- **Linux | AIX** Создайте группу и ID пользователя в домашнем каталоге пользователя, который станет владельцем экземпляра сервера.

Например, чтобы создать ID пользователя *tsminst1* в группе *tsmsrvrs* с паролем *tsminst1*, введите от имени ID административного пользователя следующие команды:

```
AIX mkgroup id=1001 tsmsrvrs
mkuser id=1002 pgrp=tsmsrvrs home=/home/tsminst1 tsminst1
passwd tsminst1
```

```
Linux groupadd tsmsrvrs
useradd -d /home/tsminst1 -m -g tsmsrvrs -s /bin/bash tsminst1
passwd tsminst1
```

Выйдите из системы, затем снова в нее войдите. Перейдите на созданную вами учетную запись пользователя. Используйте интерактивную программу входа в систему, например, *telnet*, чтобы вас попросили ввести пароль и вы смогли изменить его, если это потребуется.

- **Windows** Создайте ID пользователя, а затем добавьте новый ID в группу администраторов. Например, чтобы создать ID пользователя *tsminst1*, введите следующую команду:

```
net user tsminst1 * /add
```

После создания и проверки пароля для нового пользователя добавьте ID пользователя в группу Администраторы, введя следующие команды:

```
net localgroup Administrators tsminst1 /add
net localgroup DB2ADMNS tsminst1 /add
```

2. Завершите сеанс для нового ID пользователя.

Подготовка файловых систем для сервера

Чтобы сервер использовал дисковую систему хранения, нужно выполнить конфигурирование файловой системы.

Системы AIX

Вы должны создать группы томов, логические тома и файловые системы для сервера, используя менеджер логических томов AIX.

Процедура

1. Увеличьте глубину очереди и максимальный размер передачи для всех доступных дисков *hdiskX*. Введите для каждого диска следующие команды:

```
chdev -l hdisk4 -a max_transfer=0x1000000
chdev -l hdisk4 -a queue_depth=32
```



```
chdev -l hdisk4 -a reserve_policy=no_reserve
chdev -l hdisk4 -a algorithm=round_robin
```

Не выполняйте эти команды для внутренних дисков операционной системы, например, для *hdisk0*.

2. Создайте группы томов для базы данных, активного журнала, архивного журнала, резервного копирования базы данных и пула хранения IBM Spectrum Protect. Введите команду **mkvg**, указав ID устройств для соответствующих дисков, которые вы указали ранее.

Например, если имена устройств *hdisk4*, *hdisk5* и *hdisk6* соответствуют дискам базы данных, включите их в группу томов базы данных и т.д.

Размер системы: Приведенные ниже команды основаны на конфигурации системы среднего размера. Для малых и больших систем необходимо соответствующим образом настроить синтаксис.

```
mkvg -S -y tsmdb hdisk2 hdisk3 hdisk4
mkvg -S -y tsmactlog hdisk5
mkvg -S -y tsmarchlog hdisk6
mkvg -S -y tsmdbback hdisk7 hdisk8 hdisk9 hdisk10
mkvg -S -y tsmstgpool hdisk11 hdisk12 hdisk13 hdisk14 ... hdisk49
```

3. Определите имена физического тома и число свободных физических разделов, которые следует использовать при создании логических томов. Введите команду **lsvg** для каждой группы томов, которую вы создали в предыдущем шаге.

Например:

```
lsvg -p tsmdb
```

Вывод будет подобен следующему. В столбце *FREE PPs* представлены свободные физические разделы:

tsmdb:	PV_NAME	PV STATE	TOTAL PPs	FREE PPs	FREE DISTRIBUTION
	hdisk4	active	1631	1631	327..326..326..326..326
	hdisk5	active	1631	1631	327..326..326..326..326
	hdisk6	active	1631	1631	327..326..326..326..326

4. Создайте логические тома в каждой группе томов при помощи команды **mklv**. Размер томов, группа томов и имена устройств будут разными в зависимости от размера вашей системы и различий в конфигурации дисков.

Например, чтобы создать тома для базы данных IBM Spectrum Protect в системе среднего размера, введите следующие команды:

```
mklv -y tsmdb00 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk2
mklv -y tsmdb01 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk3
mklv -y tsmdb02 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk4
```

5. Сформатируйте файловые системы на каждом логическом томе, используя команду **crfs**.

Например, чтобы сформатировать файловые системы для базы данных в системе среднего размера, введите следующие команды:

```
crfs -v jfs2 -d tsmdb00 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace00 -A yes
crfs -v jfs2 -d tsmdb01 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace01 -A yes
crfs -v jfs2 -d tsmdb02 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace02 -A yes
```

6. Смонтируйте все заново созданные файловые системы, введя следующую команду:

```
mount -a
```

7. Вызовите список всех файловых систем, введя команду **df**.

Убедитесь, что файловые системы смонтированы с использованием правильного LUN и правильной точки монтирования. Проверьте также доступное пространство.

В следующем примере выходной информации команды показано, что объем используемого пространства, как правило, составляет 1%:

```
tapsrv07> df -g /tsminst1/*
Файловая сист. Блоки ГБ Свободно % исп. Мое исп. % моего исп. Смонтировано
/dev/tsmact00 195.12 194.59 1% 4 1% /tsminst1/TSMalog
```

8. Убедитесь, что у ID пользователя, созданного в разделе [“Создание ID пользователя для сервера”](#) на стр. 45, есть права доступа для чтения и записи к каталогам на сервере.

Системы Linux

Файловые системы ext4 или xfs следует сформатировать на каждом из LUN диска, которые будет использовать сервер IBM Spectrum Protect.

Процедура

1. Используя список ID устройств, сгенерированный ранее, введите команду **mkfs**, чтобы создать и сформатировать файловую систему для каждого устройства LUN хранения. Укажите ID устройства в команде. Смотрите следующую таблицу.
Для базы данных сформируйте файловые системы ext4:

```
mkfs -t ext4 -T largefile -m 2 /dev/mapper/36005076802810c509800000000000012
```

Для LUN пула хранения сформируйте файловые системы xfs:

```
mkfs -t xfs /dev/mapper/36005076300810105780000000000002c3
```

Команду **mkfs** можно вводить до 50 раз в зависимости от того, сколько разных устройств у вас есть.

2. Создайте каталоги точек монтирования для файловых систем.

Введите команду **mkdir** для каждого каталога, который вы должны создать. Используйте значения каталогов, записанные вами в рабочих таблицах планирования.

Например, чтобы создать каталог экземпляра сервера, используя значение по умолчанию, введите следующую команду:

```
mkdir /tsminst1
```

Повторите команду **mkdir** для каждой файловой системы.

3. Добавьте в файл `/etc/fstab` запись для каждой файловой системы, чтобы файловые системы монтировались автоматически при запуске сервера.

Например:

```
/dev/mapper/36005076802810c509800000000000012 /tsminst1/TSMdbspace00 ext4
defaults 0 0
```

4. Смонтируйте файловые системы, которые вы добавили в файл `/etc/fstab`, введя команду **mount -a**.
5. Вызовите список всех файловых систем, введя команду **df**.

Убедитесь, что файловые системы смонтированы с использованием правильного LUN и правильной точки монтирования. Проверьте также доступное пространство.

В следующем примере в системе IBM Storwize показано, что объем используемого пространства, как правило, составляет 1%:

```
[root@tapsrv04 ~]# df -h /tsminst1/*
Файловая сист.          Размер Исп. Дост. Исп. % Где
смонтир.
```

```
/dev/mapper/36005076300810105780000000000003 134G 188M 132G 1% /tsminst1/  
TSMalog
```

6. Убедитесь, что у ID пользователя, созданного в разделе [“Создание ID пользователя для сервера”](#) на стр. 45, есть права доступа для чтения и записи к каталогам на сервере IBM Spectrum Protect.

Системы Windows

Вы должны сформатировать файловые системы New Technology (NTFS) на каждом из LUN дисков, которые будут использоваться сервером IBM Spectrum Protect.

Procedure

1. Создайте каталоги точек монтирования для файловых систем.

Введите команду **md** для каждого каталога, который вы должны создать. Используйте значения каталогов, записанные вами в рабочих таблицах планирования. Например, чтобы создать каталог экземпляра сервера, используя значение по умолчанию, введите следующую команду:

```
md c:\tsminst1
```

Повторите команду **md** для каждой файловой системы.

2. Создайте том для каждого LUN диска, отображенного в каталог в каталоге экземпляра сервера с использованием менеджера томов Windows.

Выберите **Менеджер серверов > Службы файлов и хранения** и выполните описанные ниже шаги для каждого диска, соответствующего отображению LUN, созданному в предыдущем шаге:

- a) Переведите диск в подключенное состояние.
- b) Инициализируйте диск до базового типа GPT, который является типом по умолчанию.
- c) Создайте простой том, занимающий все пространство на диске. Сформируйте файловую систему с использованием NTFS и задайте метку, соответствующую назначению тома, например, TSMfile00. Не назначайте для нового тома букву диска. Вместо этого отобразите том в каталог в каталоге экземпляра, например, в C:\tsminst1\TSMfile00.

Tip: Определите метку тома и метки отображений каталога на основе сообщенного размера диска.

3. Убедитесь, что файловые системы смонтированы с использованием правильного LUN и правильной точки монтирования. Вызовите список всех файловых систем, введя команду **mountvol** и ознакомившись с выходной информацией.

Например:

```
\\?\Volume{8ffb9678-3216-474c-a021-20e420816a92}\  
C:\tsminst1\TSMdbspace00\
```

4. По завершении конфигурирования диска перезапустите систему.

What to do next

Вы можете подтвердить объем свободного пространства для каждого тома, используя Проводник Windows.

Установка сервера и компонента Центр операций

Используйте для установки компонентов графический мастер IBM Installation Manager.

Установка в системах AIX и Linux

Установите сервер IBM Spectrum Protect и Центр операций в одной и той же системе.

Прежде чем начать

Убедитесь, что для операционной системы задан нужный язык. По умолчанию язык операционной системы - это язык мастера по установке.

Процедура

1. AIX

Убедитесь, что у вас в системе установлены необходимые файлы RPM.

Дополнительные сведения смотрите в разделе [“Установка обязательных файлов RPM для графического мастера”](#) на стр. 50.

2. Прежде чем скачивать пакет установки, убедитесь, что у вас достаточно места для хранения файлов установки после их извлечения из пакета продукта.

Требования к пространству смотрите в документе по скачиванию по адресу: [Техническое замечание 588093](#).

3. Перейдите на страницу [Passport Advantage](#) и скачайте файл пакета в пустой каталог по вашему выбору.

4. Убедитесь, что для пакета заданы разрешения для выполнения. Если нужно, то измените разрешения для файла, введя следующую команду:

```
chmod a+x имя_пакета.bin
```

5. Извлеките пакет, введя следующую команду:

```
./имя_пакета.bin
```

где `имя_пакета` - это имя скачанного файла.

6. AIX

Убедитесь, что включена следующая команда, чтобы мастера работали правильно:

```
lsuser
```

По умолчанию эта команда включена.

7. Перейдите в каталог, куда вы поместили исполняемый файл.

8. Запустите мастер установки, введя следующую команду:

```
./install.sh
```

Выбирая пакеты для установки, выберите и сервер, и Центр операций.

Дальнейшие действия

- Если в процессе установки возникнут ошибки, они записываются в файлы журнала, которые хранятся в каталоге журналов IBM Installation Manager.

Чтобы просмотреть файлы журнала установки в инструменте Installation Manager, выберите **Файл > Просмотреть журнал**. Чтобы собрать эти файлы журналов из инструмента Installation Manager, выберите **Справка > Экспорт данных для анализа ошибок**.

- После установки сервера и до его настройки к работе посетите сайт [Сайт поддержки IBM Spectrum Protect](#). Щелкните по **Support and downloads** (Поддержка и материалы для скачивания) и примените все требуемые исправления.

AIX

Установка обязательных файлов RPM для графического мастера

Файлы RPM необходимы для графического мастера IBM Installation Manager.

Процедура

1. Убедитесь, что у вас в системе установлены следующие файлы: Если файлы не установлены, перейдите к шагу 2.

```
atk-1.12.3-2.aix5.2.ppc.rpm      libpng-1.2.32-2.aix5.2.ppc.rpm
cairo-1.8.8-1.aix5.2.ppc.rpm    libtiff-3.8.2-1.aix5.2.ppc.rpm
expat-2.0.1-1.aix5.2.ppc.rpm    pango-1.14.5-4.aix5.2.ppc.rpm
fontconfig-2.4.2-1.aix5.2.ppc.rpm  pixman-0.12.0-3.aix5.2.ppc.rpm
freetype2-2.3.9-1.aix5.2.ppc.rpm  xcursor-1.1.7-3.aix5.2.ppc.rpm
gettext-0.10.40-6.aix5.1.ppc.rpm  xft-2.1.6-5.aix5.1.ppc.rpm
glib2-2.12.4-2.aix5.2.ppc.rpm    xrender-0.9.1-3.aix5.2.ppc.rpm
gtk2-2.10.6-4.aix5.1.ppc.rpm      zlib-1.2.3-3.aix5.1.ppc.rpm
libjpeg-6b-6.aix5.1.ppc.rpm
```

2. Убедитесь, что в файловой системе /opt свободно, по крайней мере, 150 МБ пространства.
3. В каталоге, в который извлечен файл пакета установки, перейдите в подкаталог gtk.
4. Скачайте файлы RPM в текущий рабочий каталог с [веб-сайта IBM AIX Toolbox for Linux Applications](#), введя следующую команду:

```
download-prerequisites.sh
```

5. Установите скачанные файлы RPM в каталоге, в котором они находятся, введя следующую команду:

```
rpm -Uvh *.rpm
```

Установка в системах Windows

Установите сервер IBM Spectrum Protect и Центр операций в одной и той же системе.

Прежде чем начать

Убедитесь, что выполнены следующие обязательные требования:

- Убедитесь, что для операционной системы задан нужный язык. По умолчанию язык операционной системы - это язык мастера по установке.
- Убедитесь, что у ID пользователя, который вы планируете использовать для установки, есть полномочия локального администратора.

Процедура

1. Прежде чем скачивать пакет установки, убедитесь, что у вас достаточно места для хранения файлов установки после их извлечения из пакета продукта.
Требования к пространству смотрите в документе по скачиванию по адресу: [Техническое замечание 588095](#).
2. Перейдите на страницу [Passport Advantage](#) и скачайте файл пакета в пустой каталог по вашему выбору.
3. Перейдите в каталог, куда вы поместили исполняемый файл.
4. Дважды щелкните по выполняемому файлу, чтобы извлечь его в текущий каталог.
5. В каталоге, куда были распакованы файлы установки, запустите мастер установки, дважды щелкнув по файлу `install.bat`.
Выбирая пакеты для установки, выберите и сервер, и Центр операций.

Дальнейшие действия

- Если в процессе установки возникнут ошибки, они записываются в файлы журнала, которые хранятся в каталоге журналов IBM Installation Manager.

Чтобы просмотреть файлы журнала установки в инструменте Installation Manager, выберите **Файл > Просмотреть журнал**. Чтобы собрать эти файлы журналов из инструмента Installation Manager, выберите **Справка > Экспорт данных для анализа ошибок**.

- После установки сервера и до его настройки к работе посетите сайт [Сайт поддержки IBM Spectrum Protect](#). Щелкните по **Support and downloads** (Поддержка и материалы для скачивания) и примените все требуемые исправления.

Конфигурирование сервера и компонента Центр операций

После установки компонентов выполните конфигурирование сервера IBM Spectrum Protect и компонента Центр операций.

Конфигурирование экземпляра сервера

Используйте мастер конфигурирования экземпляра сервера IBM Spectrum Protect, чтобы выполнить первоначальное конфигурирование сервера.

Прежде чем начать

Убедитесь, что выполнены следующие требования:

Linux | AIX

- В системе, в которой вы установили IBM Spectrum Protect, должен быть клиент X Window System. Кроме того, у вас на рабочем столе должен работать сервер X Window System.
- В системе должен быть разрешен протокол Secure Shell (SSH). Убедитесь, что для порта задано значение по умолчанию (22) и что порт не заблокирован брандмауэром. Нужно разрешить аутентификацию пароля в файле `sshd_config` в каталоге `/etc/ssh/`. Убедитесь также, что у службы демона SSH есть права доступа для соединения с системой с использованием значения `localhost`.
- Вы должны иметь возможность войти в IBM Spectrum Protect, используя ID пользователя, созданный для экземпляра сервера, и протокол SSH. При использовании мастера для получения доступа к системе вы должны будете ввести эти ID пользователя и пароль.
- Если вы изменили какие-либо параметры в предыдущих шагах, перезапустите сервер, прежде чем приступить к работе с мастером конфигурирования.

Windows

Убедитесь, что служба удаленного реестра запущена, выполнив следующие шаги:

1. Выберите **Пуск > Администрирование > Службы**. В окне **Службы** выберите **Удаленный реестр**. Если служба не запущена, щелкните по **Пуск**.
2. Убедитесь, что порты 137, 139 и 445 не заблокированы брандмауэром:
 - a. Щелкните по **Запуск > Панель управления > Брандмауэр Windows**.
 - b. Выберите **Дополнительные параметры**.
 - c. Выберите **Входные правила**.
 - d. Выберите **Новое правило**.
 - e. Создайте правило порта для портов TCP 137, 139 и 445, чтобы разрешить соединения для доменных и частных сетей.
3. Сконфигурируйте управление учетными записями пользователей, получив доступ к опциям Локальная политика безопасности и выполнив следующие шаги:
 - a. Щелкните по **Пуск > Администрирование > Локальная политика безопасности**. Разверните **Локальные политики > Опции безопасности**.

- b. Если эта возможность еще не включена, включите встроенную учетную запись администратора, выбрав **Учетные записи: Состояние учетной записи администратора > Включить > ОК**.
 - c. Если эта возможность еще не выключена, выключите управление учетными записями пользователей для всех администраторов Windows, выбрав **Управление учетными записями пользователей: Запускать всех администраторов в режиме утверждения администраторов > Выключить > ОК**.
 - d. Если эта возможность еще не выключена, выключите управление учетными записями пользователей для встроенной учетной записи администратора, выбрав **Управление учетными записями пользователей: Режим утверждения администраторов для встроенной учетной записи администратора > Выключить > ОК**.
4. Если вы изменили какие-либо параметры в предыдущих шагах, перезапустите сервер, прежде чем приступить к работе с мастером конфигурирования.

Об этой задаче

Мастер можно останавливать и перезапускать, но сервер не будет работать, пока не будет выполнена вся процедура конфигурирования.

Процедура

1. Запустите локальную версию мастера.

- **Linux | AIX** Откройте программу dsmicfgx в каталоге /opt/tivoli/tsm/server/bin. Этот мастер можно запустить только от имени пользователя root.
- **Windows** Выберите **Пуск > Все программы > IBM Spectrum Protect > Мастер конфигурирования**.

2. Завершите конфигурирование, следуя инструкциям.

Используйте информацию, записанную вами в таблицу “Рабочие листы планирования” на стр. 8 в ходе настройки системы IBM Spectrum Protect, чтобы задать каталоги и опции в мастере.

Linux | AIX В окне **Информация о сервере** задайте автоматический запуск сервера при загрузке системы, используя ID пользователя экземпляра.

Windows При использовании мастера конфигурирования для сервера будет задан автоматический запуск при перезагрузке.

Установка клиента резервного копирования и архивирования

Лучше всего установить клиент резервного копирования и архивирования IBM Spectrum Protect в серверной системе, чтобы были доступны административный клиент командной строки и планировщик.

Procedure

- Чтобы установить клиент резервного копирования и архивирования, выполните инструкции по установке для вашей операционной системы.
 - [Установить клиентов резервного копирования и архивирования UNIX и Linux](#)
 - [Первая установка клиента Windows](#)

Как задать опции для сервера

Проверьте файл опций сервера, установленный вместе с сервером IBM Spectrum Protect, чтобы убедиться, что заданы правильные значения для вашей системы.

Процедура

1. Перейдите в каталог экземпляра сервера и откройте файл dsmserve.opt.

2. Ознакомьтесь со следующими значениями в таблице и проверьте параметры опций сервера на основе размера системы.

Серверный параметр	Значение
ACTIVELOGDIRECTORY	Путь каталога, заданный во время конфигурации
ACTIVELOGSIZE	131072
ARCHLOGCOMPRESS	Нет
ARCHLOGDIRECTORY	Путь каталога, заданный во время конфигурации
COMMMETHOD	TCP/IP
COMMTIMEOUT	3600
DEVCONFIG	devconf.dat
EXPINTERVAL	0
IDLETIMEOUT	60
MAXSESSIONS	500
NUMOPENVOLSALLOWED	20
TCPADMINPORT	1500
TCPPORT	1500
VOLUMEHISTORY	volhist.dat

Обновите параметры опций сервера, если потребуется, чтобы они соответствовали значениям в таблице. Чтобы внести обновления, закройте файл `dsmsevr.opt` и воспользуйтесь командой **SETOPT** в интерфейсе командной строки администрирования, чтобы задать опции.

Например, чтобы обновить опцию `IDLETIMEOUT` до 60, введите следующую команду:

```
setopt idletimeout 60
```

3. Чтобы сконфигурировать защищенную связь с сервером, клиентами и Центром операций, проверьте опции в следующей таблице:

Серверный параметр	Системы всех размеров
SSLDISABLELEGACYTLS	YES
SSLFIPSMODE	NO
SSLTCPPORT	Задайте номер порта SSL. Драйвер связи TCP/IP сервера ожидает на этом порту поступления от клиента требований об установлении сеансов с поддержкой SSL.
SSLTCPADMINPORT	Задайте адрес порта, на котором сервер ожидает требований установления сеансов SSL от клиента администрирования с интерфейсом командной строки.
TLS12	YES

Если нужно обновить любое из значений опций, измените файл `dsmsevr.opt`, используя следующие рекомендации:

- Чтобы включить опцию, удалите звездочку в начале строки.
- В каждой строке введите только одну опцию и заданное для нее значение.

- Если опция встречается в нескольких записях в файле, сервер будет использовать последнюю запись.

Сохраните свои изменения файл и закройте файл. Если вы непосредственно внесете изменения в файл `dsmsevr.opt`, вы должны будете перезапустить сервер, чтобы изменения вступили в силу.

Понятия, касающиеся защиты

Вы можете защитить IBM Spectrum Protect от рисков защиты, используя протоколы связи, защиту паролей и предоставляя администраторам разные уровни доступа.

Transport Layer Security

Можно использовать протокол Secure Sockets Layer (SSL) или Transport Layer Security (TLS), чтобы обеспечить защиту транспортного слоя для безопасной связи между серверами, клиентами и агентами хранения. Если вы пересылаете данные между сервером, клиентом и агентом хранения, используйте SSL или TLS для шифрования данных.

Совет: Любая документация IBM Spectrum Protect, обозначенная как "SSL" или "выбрать SSL", применима к TLS.

SSL предоставляется Global Security Kit (GSKit), установленным с сервером IBM Spectrum Protect и используемым сервером, клиентом и агентом хранения.

Ограничение: Не используйте протоколы SSL и TLS для связи с экземпляром базы данных IBM Db2, который используется какими-либо серверами IBM Spectrum Protect.

Каждый сервер, клиент или агент хранения, на котором включается поддержка SSL, должен использовать доверенный самоподписанный сертификат или получить уникальный сертификат, подписанный сертификатом (certificate authority, CA). Вы можете использовать свои собственные сертификаты или можете приобрести сертификаты у сертификатора (CA). Любой сертификат нужно установить и добавить к базе данных ключей для сервера IBM Spectrum Protect, клиента или агента хранения. Сертификат проверяется клиентом или сервером SSL, который затребовал или инициировал связь по SSL. Некоторые сертификаты сертификаторов предварительно устанавливаются в базах данных ключей по умолчанию.

SSL устанавливается независимо от сервера IBM Spectrum Protect, клиента и агента хранения.

Уровни полномочий

При использовании каждого сервера IBM Spectrum Protect существует ряд доступных уровней административных полномочий, определяющих задачи, которые может выполнить администратор.

После регистрации администратору нужно предоставить полномочия, назначив для него один или несколько уровней административных полномочий. Администратор с системными полномочиями может выполнить любую задачу с сервером и назначить уровни полномочий для других администраторов, воспользовавшись командой **GRANT AUTHORITY**. Администраторы, обладающие полномочиями политики, хранения или оператора, могут выполнять только определенный набор задач.

Администратор может зарегистрировать другие ID администраторов, предоставить им уровни полномочий, переименовать или удалить их, а также блокировать или разблокировать их доступ к серверу.

Администратор может управлять доступом к определенным клиентским узлам для ID пользователей root и ID пользователей, не являющихся пользователями root. По умолчанию, ID пользователя, не являющегося пользователем root, не может производить резервное копирование данных на узле. Используйте команду **UPDATE NODE**, чтобы изменить параметры узла и включить резервное копирование.

Пароли

По умолчанию сервер автоматически использует аутентификацию с помощью пароля. Если аутентификация пароля включена (on), все пользователи при получении доступа к серверу должны указывать пароль.

Используйте Lightweight Directory Access Protocol (LDAP), чтобы применить более строгие требования к паролям. Дополнительную информацию смотрите в разделе [Управление паролями и процедурами входа \(V7.1.1\)](#).

Таблица 14. Характеристики аутентификации паролей	
Характеристика	Дополнительная информация
Значение регистра символов	Без учета регистра.
Срок действия пароля по умолчанию	90 дней. Отсчет начинается с момента первой регистрации на сервере ID администратора или клиентского узла. Если в течение этого периода пароль не изменится, пароль нужно будет изменить, когда пользователь в следующий раз получит доступ к серверу.
Число попыток ввода неправильного пароля	Для всех клиентских узлов можно установить максимальное количество последовательных попыток неправильного ввода пароля. После превышения данного значения сервер блокирует такой узел.
Длина пароля по умолчанию	8 символов Администратор может задать минимальную длину. Начиная с версии 8.1.4, минимальная длина паролей сервера по умолчанию изменилась с 0 до 8 символов.

Защита сеанса

Защита сеанса - это уровень защиты, который используется для взаимодействий между узлами-клиентами IBM Spectrum Protect, клиентами администрирования и серверами и назначается с использованием параметра **SESSIONSECURITY**.

Для параметра **SESSIONSECURITY** можно задать одно из следующих значений:

- Значение **STRICT** принудительно применяет наиболее высокий уровень защиты взаимодействий между серверами IBM Spectrum Protect, узлами и администраторами.
- Значение **TRANSITIONAL** указывает, что при обновлении программы IBM Spectrum Protect до V8.1.2 или новее используется существующий протокол связи. Это значение по умолчанию. Если задано **SESSIONSECURITY=TRANSITIONAL**, автоматически применяются более строгие параметры защиты при использовании более высоких версий протокола TLS и при обновлении программы до V8.1.2 или новее. После того как узел, администратор или сервер будет соответствовать требованиям для значения **STRICT**, защита сеанса автоматически обновится до значения **STRICT**, и объект больше не сможет проходить аутентификацию, используя предыдущую версию клиента или более ранние протоколы TLS.

Прим.: До обновления серверов обновлять клиенты резервного копирования и архивирования до V8.1.2 или новее не нужно. После обновления сервера до V8.1.2 или новее узлы и администраторы, использующие более ранние версии программы, продолжают взаимодействовать с сервером, используя значение **TRANSITIONAL**, пока объект будет соответствовать требованиям для значения **STRICT**. Точно так же можно обновить клиенты

резервного копирования и архивирования до V8.1.2 или новее до обновления серверов IBM Spectrum Protect, но обновлять серверы сначала не требуется. Связь между серверами и клиентами не прерывается.

Дополнительные сведения о значениях параметра **SESSIONSECURITY** смотрите в описаниях следующих команд.

Таблица 15. Команды, используемые, чтобы задать параметр SESSIONSECURITY	
Объект	Команда
Клиентские узлы	<ul style="list-style-type: none">• REGISTER NODE• UPDATE NODE
Администраторы	<ul style="list-style-type: none">• REGISTER ADMIN• UPDATE ADMIN
Серверы	<ul style="list-style-type: none">• DEFINE SERVER• UPDATE SERVER

Администраторы, прошедшие аутентификацию с использованием команды **DSMADMC**, команды **DSMC** или программы dsm, после аутентификации с использованием V8.1.2 или новее не смогут проходить аутентификацию с использованием более ранней версии. Чтобы устранить проблемы аутентификации администраторов, смотрите следующие советы:

Советы:

- Убедитесь, что все программы IBM Spectrum Protect, используемые учетной записью администратора для входа в систему, обновлены до V8.1.2 или новее. Если учетная запись администратора производит вход из нескольких систем, убедитесь, что сертификат сервера установлен в каждой системе.
- После того, как администратор успешно аутентифицируется на сервере с использованием программного обеспечения V8.1.2 или более новой версии, или V7.1.8 или более новой версии, администратор больше не сможет пройти аутентификацию на этом сервере, используя версии клиента или сервера более ранней версии, чем V8.1.2 или V7.1.8. Команду администратора можно вводить из любой системы.
- Если потребуется, создайте отдельную учетную запись администратора, чтобы использовать ее только при работе с клиентами и серверами, на которых работает V8.1.1 или более ранняя программа.

Принудительно примените наивысший уровень защиты взаимодействий с сервером IBM Spectrum Protect, сделав так, чтобы все узлы, администраторы и серверы использовали защиту сеанса STRICT. Можно воспользоваться командой **SELECT** чтобы определить, какие серверы, узлы и администраторы используют защиту сеанса TRANSITIONAL, чтобы их обновить для использования защиты сеанса STRICT.

Информация, связанная с данной

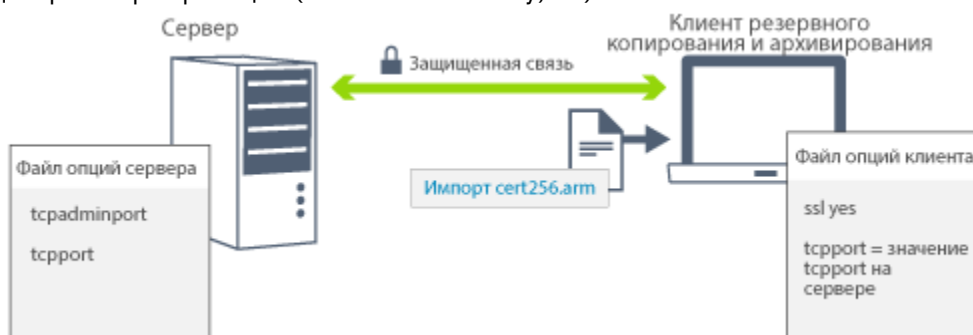
[Защита связи](#)

Конфигурирование защищенной связи с использованием Transport Layer Security (TLS)

Чтобы шифровать данные и защищать связь в вашей среде, на сервере и на клиенте резервного копирования и архивирования IBM Spectrum Protect включен протокол Secure Sockets Layer (SSL) или Transport Layer Security (TLS). Сертификат SSL используется для проверки требований связи между сервером и клиентом.

About this task

Как показано на следующем рисунке, вы можете вручную сконфигурировать защищенную связь между сервером и клиентом резервного копирования и архивирования, задав опции в файлах опций сервера и клиента, а затем перенеся на клиент самоподписанный сертификат, сгенерированный на сервере. Либо можно получить уникальный сертификат, подписанный центром сертификации (certificate authority, CA).



Дополнительную информацию о конфигурировании сервера и клиентов для взаимодействий SSL или TLS смотрите в разделе [Конфигурирование агентов хранения, серверов, клиентов и Центра операций для соединения с сервером с использованием SSL](#).

Конфигурирование Центра операций

После установки компонента Центр операций выполните описанные ниже действия по конфигурированию, чтобы начать управлять средой хранения.

Прежде чем начать

Если вы подключаетесь к компоненту Центр операций впервые, вы должны предоставить следующую информацию:

- Информация о соединении для сервера, который вы хотите назначить хаб-сервером
- Идентификационные данные входа в систему для администратора, который задан для этого сервера

Процедура

1. Определите хаб-сервер.

Введите в окне веб-браузера следующий адрес:

```
https://имя_хоста:защищенный_порт/oc
```

Здесь используются следующие обозначения:

- *имя_хоста* - это имя компьютера, где установлен компонент Центр операций
- *защищенный_порт* - это номер порта, используемого компонентом Центр операций для HTTPS-взаимодействий на этом компьютере

Например, если имя хоста - это `tsm.storage.mylocation.com` и вы используете для компонента Центр операций защищенный порт по умолчанию, адрес пример следующий вид:

```
https://tsm.storage.mylocation.com:11090/oc
```

Когда вы впервые входите в компонент Центр операций, мастер поможет вам выполнить первоначальное конфигурирование, чтобы задать нового администратора с системными полномочиями на сервере.

2. Настройте защищенные взаимодействия между компонентом Центр операций и хаб-сервером, сконфигурировав протокол Secure Sockets Layer (SSL).

Следуйте инструкциям в разделе [“Защита связи между компонентом Центр операций и хаб-сервером”](#) на стр. 59.

3. Необязательно: Чтобы ежедневно получать по электронной почте отчет, в котором суммируется состояние системы, сконфигурируйте параметры электронной почты в компоненте Центр операций.

Следуйте инструкциям в разделе [“Состояние системы отслеживания с использованием отчетов по электронной почте”](#) на стр. 165.

Защита связи между компонентом Центр операций и хаб-сервером

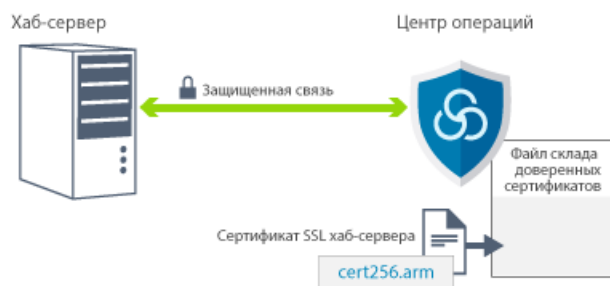
Для защиты связи между компонентом Центр операций и хаб-сервером добавьте сертификат Transport Layer Security (TLS) хаб-сервера в файл доверенного хранилища компонента Центр операций.

Before you begin

Файл доверенного склада компонента Центр операций - это контейнер сертификатов, доступ к которому может получить Центр операций. Он содержит сертификат, который Центр операций использует для связи HTTPS с веб-браузерами.

При установке компонента Центр операций вы создаете пароль для файла склада доверенных сертификатов. Чтобы защитить связь между компонентом Центр операций и хаб-сервером, нужно использовать тот же пароль для добавления сертификата хаб-сервера в файл доверенного склада. Если вы не помните этот пароль, вы можете его переустановить.

На следующем рисунке показаны компоненты для настройки SSL между компонентом Центр операций и хаб-сервером.



About this task

В этой процедуре описаны шаги по реализации защищенной связи с использованием самоподписанных сертификатов.

Procedure

Чтобы настроить связь SSL с использованием самоподписанных сертификатов, сделайте следующее:

1. Задайте сертификат `cert256.arm` в качестве сертификата по умолчанию в файле базы данных ключей хаб-сервера:

- a) Находясь в каталоге экземпляра хаб-сервера, введите следующую команду:

```
gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed
-label "TSM Server SelfSigned SHA Key"
```

- b) Перезапустите хаб-сервер, чтобы он получил изменения, внесенные в файл базы данных ключей.

- c) Убедитесь, что сертификат `cert256.arm` задан как сертификат по умолчанию. Введите следующую команду:

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

2. Остановите веб-сервер Центра операций.
3. Откройте командную строку операционной системы в системе, где установлен компонент Центр операций, и перейдите в следующий каталог:

- **Linux** | **AIX** `каталог_установки/ui/jre/bin`
- **Windows** `каталог_установки\ui\jre\bin`

Где `каталог_установки` - это каталог, в котором установлен компонент Центр операций.

4. Откройте окно Управление ключами IBM, введя следующую команду:

```
ikeyman
```

5. Выберите **Файл базы данных ключей > Открыть**.
6. Щелкните по **Обзор** и перейдите в следующий каталог, где `каталог_установки` - это каталог, в котором установлен компонент Центр операций:
7. Выберите в каталоге `guiServer` файл `gui-truststore.jks`.
8. Щелкните по **Открыть**, а затем по **ОК**.
9. Введите пароль для файла доверенного склада и щелкните по **ОК**.
10. В области Контент базы данных ключей окна Управление ключами IBM щелкните по стрелке и выберите в списке **Сертификаты подписывающих**. Щелкните по **Добавить**.
11. В окне Открыть щелкните по **Обзор** и перейдите в каталог экземпляра хаб-сервера:

- **Linux** | **AIX** `/opt/tivoli/tsm/server/bin`
- **Windows** `с:\Program Files\Tivoli\TSM\server1`

В каталоге содержится сертификат `cert256.arm`.

Если из окна Открыть недоступен каталог экземпляра хаб-сервера, выполните следующие действия:

- a) При помощи FTP или другого способа передачи файлов скопируйте файлы `cert256.arm` с хаб-сервера в следующий каталог на компьютере, на котором установлен компонент Центр операций:

- **Linux** | **AIX** `каталог_установки/ui/Liberty/usr/servers/guiServer`
- **Windows** `каталог_установки\ui\Liberty\usr\servers\guiServer`

- b) В окне Открыть перейдите в каталог `guiServer`.

12. Выберите сертификат `cert256.arm` в качестве сертификата SSL.
13. Щелкните по **Открыть**, а затем по **ОК**.
14. Введите метку для сертификата. Например, задайте имя хаб-сервера.
15. Щелкните по **ОК**. Сертификат SSL хаб-сервера добавлен в файл доверенного хранилища, и его метка выводится в области Содержимое базы данных ключей окна Управление ключами IBM.
16. Закройте окно Управление ключами IBM.
17. Запустите веб-сервер Центра операций.

Когда вы в первый раз будете соединяться с компонентом Центр операций, вас попросят указать IP-адрес или сетевое имя хаб-сервера и номер порта для связи с хаб-сервером. Если опция сервера `ADMINONCLIENTPORT` включена для сервера IBM Spectrum Protect, введите номер порта, заданный опцией сервера `TCPADMINPORT`. Если опция сервера `ADMINONCLIENTPORT` не включена, введите номер порта, заданный опцией сервера `TCPPORT`.

Регистрация лицензии на продукт


Чтобы зарегистрировать лицензию для продукта IBM Spectrum Protect, используйте команду **REGISTER LICENSE**.

About this task

Лицензии хранятся в файлах сертификата регистрации, который содержит сведения о лицензировании для продукта. Файлы регистрационных сертификатов находятся на носителе установки и при установке помещаются на сервер. После регистрации продукта лицензии хранятся в NODELOCK-файле в текущем каталоге.

Procedure


Зарегистрируйте лицензию, указав имя файла сертификата регистрации, содержащего лицензию. Чтобы использовать построитель команд Центра операций для этой задачи, выполните следующие шаги:

1. Откройте Центр операций.
2. Откройте построитель команд компонента Центр операций, установив указатель мыши на значок параметров  и щелкнув по **Построитель команд**.
3. Введите команду **REGISTER LICENSE**.
Например, чтобы зарегистрировать базовую лицензию IBM Spectrum Protect, введите следующую команду:

```
register license file=tsmbasic.lic
```

What to do next

Сохраните носитель установки, на котором содержатся файлы сертификата регистрации. Возможно, вам придется снова зарегистрировать лицензию, если, например, возникнет одно из следующих условий:

- Сервер перенесен на другой компьютер;
- Файл NODELOCK поврежден. Сервер сохраняет данные лицензий в файле NODELOCK, расположенном в каталоге, из которого запускается сервер.
-  **Linux** Вы изменяете микросхему процессора, связанную с сервером, на котором установлен сервер.

Как задать правила хранения данных для вашего бизнеса

После создания пула хранения каталога-контейнера для дедупликации данных обновите политику сервера по умолчанию, чтобы использовать новый пул хранения. В мастере **Добавить пул хранения** откроется страница **Службы** в компоненте Центр операций, чтобы можно было выполнить эту задачу.

Procedure

1. На странице **Службы** в Центре операций выберите домен STANDARD и щелкните по **Сведения**.
2. На странице **Сводка** для домена политики щелкните по вкладке **Наборы политики**.
На странице **Наборы политик** указано имя активного набора политики и перечислены все классы управления для этого набора политик.
3. Щелкните по переключателю **Конфигурировать** и внесите следующие изменения:
 - Измените объект назначения резервного копирования для класса управления STANDARD, задав пул хранения каталога-контейнера.
 - Измените значение в столбце Резервные копии на **Без ограничения**.

- Измените срок хранения. Задайте в столбце Хранить лишние резервные копии значение 30 дней или более в зависимости от ваших бизнес-требований.
4. Сохраните изменения и щелкните по переключателю **Конфигурировать**, чтобы набор политик стал недоступен для изменения.
 5. Активируйте набор политик, для чего щелкните по **Активировать**.

Как задать расписания для операций по обслуживанию сервера

Создайте расписания для каждой операции по обслуживанию сервера, используя команду **DEFINE SCHEDULE** в построителе команд компонента Центр операций.

Об этой задаче

Запланируйте операции обслуживания сервера, так чтобы они выполнялись после операций резервного копирования клиента. Вы можете управлять синхронизацией расписаний, задав время начала в сочетании с длительностью каждой операции.

На следующем рисунке приводится пример того, как спланировать операции обслуживания.

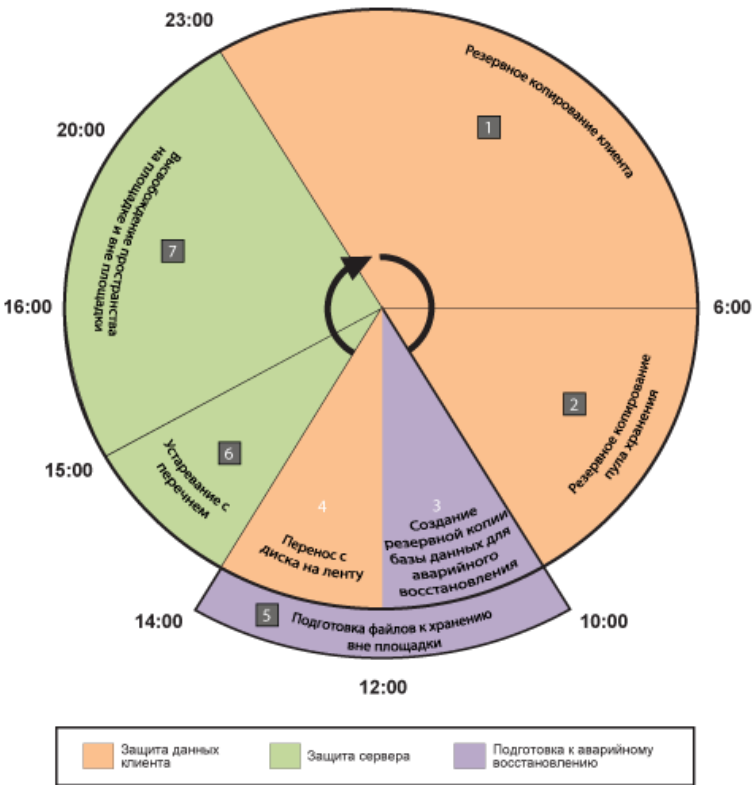


Рисунок 4. Ежедневное расписание операций сервера для решения на лентах

В приведенной ниже таблице показано, как можно запланировать процессы обслуживания сервера в сочетании с расписанием резервного копирования клиента для решения на лентах.

Операция	Запланированное задание
Резервное копирование клиента	Начинается в 23:00.

Операция	Запланированное задание
Резервное копирование пула хранения	Начинается в 06:00.
Обработка базы данных и файлов аварийного восстановления	<ul style="list-style-type: none"> Операция резервного копирования базы данных начинается в 10:00 или через 11 часов после начала операции резервного копирования клиента. Этот процесс выполняется до его завершения. Информация о конфигурации устройства и резервное копирование хронологии томов запускаются в 17:00 или спустя 7 часов после запуска операций резервного копирования базы данных. Удаление хронологии томов запускается в 20:00 или спустя 10 часов после запуска операции резервного копирования базы данных.
Подготовка файлов для хранения вне площадки	Начинается в 10:00, одновременно с началом обработки базы данных и файлов аварийного восстановления.
Перенастройка с диска для записи на ленту	Начинается в 12:00 или через 2 часа после запуска операции резервного копирования базы данных.
Устаревание инвентарного перечня	Начинается в 14:00 или через 15 часов после начала операции резервного копирования клиента. Этот процесс выполняется до его завершения.
Восстановление пространства	Начинается в 15:00 или через 16 часов после начала операции резервного копирования клиента.

Процедура

После того как вы сконфигурируете класс устройств для резервных копий базы данных, создайте расписания для резервного копирования базы данных и других необходимых операций обслуживания, используя команду **DEFINE SCHEDULE**. В зависимости от размера вашей среды вам, возможно, придется скорректировать время запуска для каждого расписания в примере.

1. Задайте класс устройств для операции резервного копирования, прежде чем создавать расписание для резервного копирования базы данных.

Используйте команду **DEFINE DEVCLASS**, чтобы создать класс устройств с именем LTOTAPE:

```
define devclass ltotape devtype=lto library=ltolib
```

2. Задайте класс устройств для автоматического резервного копирования базы данных. Используйте команду **SET DBRECOVERY**, чтобы указать класс устройств, созданный вами для резервного копирования базы данных в предыдущем шаге. Например, если класс устройств - это LTOTAPE, введите следующую команду:

```
set dbrecovery ltotape
```

3. Создайте расписания для операций обслуживания, используя команду **DEFINE SCHEDULE**. Обязательные операции с примерами команд смотрите в следующей таблице.

Операция	Примеры команд и дополнительная информация
Создайте резервные копии пулов хранения.	<p>Создайте расписание, чтобы выполнить команду BACKUP STGPOOL.</p> <p>Например, введите следующую команду, чтобы создать расписание резервного копирования для первичного пула хранения с именем PRIMARY_POOL. Резервное копирование пула будет производиться в пул хранения копий, COPYSTG:</p> <pre>define schedule BACKUPSTGPOOL type=administrative cmd="backup stgpool primary_pool copystg" active=yes starttime=06:00 period=1</pre>
Создайте резервную копию базы данных.	<p>Создайте расписание, чтобы выполнить команду BACKUP DB.</p> <p>Например, введите следующую команду, чтобы создать расписание резервного копирования, использующее новый класс устройств:</p> <pre>define schedule DBBACKUP type=admin cmd="backup db devclass=ltotape type=full numstreams=3 wait=yes compress=yes" active=yes desc="Создать рез. копию базы данных." startdate=today starttime=10:00:00 duration=45 durunits=minutes</pre>
Реплицируйте узлы.	<p>(Необязательно) Используйте репликацию узлов для защиты данных клиентов путем резервного копирования данных на вторичный сервер. Инструкции смотрите в разделе Репликация данных клиента на другой сервер. Прежде чем приступить к операциям по переносу, убедитесь, что репликация узлов выполнена.</p>

Операция	Примеры команд и дополнительная информация
<p>Переносите данные с диска на ленту ежедневно.</p>	<p>Создайте расписание для переноса пула хранения.</p> <p>Например, если имя дискового пула хранения - DISKPOOL, а имя следующего пула хранения - TAPEPOOL, вы можете запланировать перенос пула хранения, введя следующую команду:</p> <pre>define schedule stgpool_migration type=administrative cmd="migrate stgpool diskpool lomig=0" active=yes description="migrate disk storagepool to tapepool" startdate=today starttime=12:00 duration=2 durunits=hours period=1 perunits=days</pre> <p>Чтобы довести пропускную способность до максимума, можно задать число параллельных процессов, которые следует использовать для переноса файлов, выполнив следующие шаги:</p> <ol style="list-style-type: none"> В случае ленточного пула хранения убедитесь, что включено совместное размещение. Чтобы проверить, включено ли совместное размещение, введите команду QUERY STGPOOL. Убедитесь, что в поле COLLOCATE задано значение GROUP, NODE или FILESPACE. Если значение GROUP, NODE или FILESPACE не задано, используйте команду UPDATE STGPOOL, чтобы задать COLLOCATE=GROUP, COLLOCATE=NODE или COLLOCATE=FILESPACE в зависимости от конфигурации вашей системы. Для дискового пула хранения используйте команду DEFINE STGPOOL или UPDATE STGPOOL, чтобы задать значение для параметра MIGPROCESS. Например, если у вас есть 12 ленточных накопителей, задайте MIGPROCESS=10. Таким образом для процессов переноса будет использоваться число ленточных накопителей, достигающее 10. Два накопителя резервируются для других задач, например, операций восстановления, резервного копирования базы данных и резервного копирования клиента.
<p>Подготовьте файлы для хранения вне площадки.</p>	<ol style="list-style-type: none"> Переместите ленточные тома куда-либо вне площадки, следуя инструкциям в разделе “Перемещение носителей резервных копий” на стр. 67. Создайте файл плана аварийного восстановления, введя команду PREPARE на исходном сервере: <pre>prepare</pre> <ol style="list-style-type: none"> Убедитесь, что все тома, которые требуются для восстановления после аварий, включены в файл плана восстановления. Дополнительную информацию смотрите в разделе “Подготовка к аварии и восстановление после аварии с использованием DRM” на стр. 225.
<p>Создайте резервную копию информации о конфигурации устройств.</p>	<p>Создайте расписание, чтобы выполнить команду BACKUP DEVCONFIG:</p> <pre>define schedule DEVCONFIGBKUP type=admin cmd="backup devconfig filenames=devconfig.dat" active=yes desc="Создать рез. копию файла конфигурации устройства." startdate=today starttime=17:00:00 duration=45 durunits=minutes</pre>

Операция	Примеры команд и дополнительная информация
Создайте резервную копию хронологии томов.	<p>Создайте расписание, чтобы выполнить команду BACKUP VOLHISTORY:</p> <pre>define schedule VOLHISTBKUP type=admin cmd="backup volhistory filenames=volhist.dat" active=yes desc="Создать резервную копию хронологии томов." startdate=today starttime=17:00:00 duration=45 durunits=minutes</pre>
Удалите более старые версии резервных копий базы данных, которые больше не требуются.	<p>Создайте расписание, чтобы выполнить команду DELETE VOLHISTORY:</p> <pre>define schedule DELVOLHIST type=admin cmd="delete volhistory type=dbb todate=today-6 totime=now" active=yes desc="Удалить старые резервные копии базы данных." startdate=today starttime=20:00:00 duration=45 durunits=minutes</pre>
Удалите объекты, у которых превышен допустимый срок хранения.	<p>Создайте расписание, чтобы выполнить команду EXPIRE INVENTORY.</p> <p>Задайте параметр RESOURCE на основе размера системы, которую вы конфигурируете, так чтобы он был равен числу ядер процессора, заданному вами для вашей системы.</p> <p>Например, введите следующую команду, чтобы создать расписание с именем EXPINVENTORY:</p> <pre>define schedule EXPINVENTORY type=admin cmd="expire inventory wait=yes resource=8 duration=120" active=yes desc="Удалить проср. объекты." startdate=today starttime=14:00:00 duration=1 durunits=hours</pre>
Высвободите пространство.	<p>Создайте расписание, чтобы выполнить команду RECLAIM STGPPOOL.</p> <p>Например, введите следующую команду, чтобы создать расписание с именем RECLAIM:</p> <pre>define schedule RECLAIM type=admin cmd="reclaim stgpool tapepool duration=60" startdate=today starttime=15:00:00 duration=5 durunits=hours</pre> <p>Совет: Чтобы довести пропускную способность до максимума, можно задать число параллельных процессов, которые следует использовать для освобождения пространства. Обновите пул хранения на ленте, используя команду UPDATE STGPPOOL, и задайте значение для параметра RECLAIMPROCESS. Например, если у вас есть 12 ленточных накопителей, задайте RECLAIMPROCESS=5. Поскольку для каждого процесса освобождения используются два накопителя, общее число накопителей, которые могут использоваться для восстановления, равно 10. Два накопителя зарезервированы для операций резервного копирования.</p>

Дальнейшие действия

После того как вы создадите расписания задач по обслуживанию сервера, вы сможете увидеть их в компоненте Центр операций, выполнив следующие шаги:

1. В строке меню Центра операций наведите указатель мыши на **Серверы**.
2. Щелкните по **Обслуживание**.

Информация, связанная с данной

[UPDATE STGPOOL \(обновить пул хранения\)](#)

[DEFINE SCHEDULE \(определение расписания выполнения административных команд\)](#)

[DEFINE STGPOOL \(определение тома в пуле хранения\)](#)

Перемещение носителей резервных копий

Для восстановления после аварии необходимы тома с резервными копиями базы данных, тома пулов хранения копий и дополнительные файлы. Чтобы быть готовым к аварийной ситуации, нужно выполнять ежедневные задачи.

Прежде чем начать

Чтобы увидеть все тома пула хранения виртуальных копий и резервных копий базы данных, у которых есть объекты резервных копий на удаленном сервере назначения, введите команду **QUERY DRMEDIA:**

```
query dimedia * wherestate=remote
```

Об этой задаче

На следующем рисунке показан жизненный цикл типичной операции, чтобы переместить резервные носители вне площадки и обратно на площадку как часть операций по аварийному восстановлению.



Рисунок 5. Жизненный цикл носителя для восстановления

Менеджер аварийного восстановления (DRM) назначает следующие состояния носителя на тома. Состояния носителя отслеживают том, когда он перемещается из расположения в расположение.

Некоторые состояния носителей необязательные. В зависимости от того, насколько хорошо ваша организация хочет отслеживать перемещения тома, ваша организация может пропустить эти необязательные состояния носителей.

MOUNTABLE

Том содержит актуальные данные, находится на площадке, и сервер IBM Spectrum Protect может получить к нему доступ.

NOTMOUNTABLE

Том содержит актуальные данные и подключен, но сервер IBM Spectrum Protect не может получить к нему доступ.

COURIER

Том содержит актуальные данные и находится на пути в помещение хранения.

VAULT

Том содержит актуальные данные и находится в помещении хранения.

VAULTRETRIEVE

Том, расположенный вне площадки, больше не содержит актуальных данных и должен быть возвращен на площадку.

COURIERRETRIEVE

Том больше не содержит актуальных данных и находится у курьера.

ONSITERETRIEVE

Том больше не содержит актуальных данных и возвращается на площадку. Записи о томах резервной копии базы данных, чистых томах пулов хранения копий и чистых томах пулов активных данных удалены из базы данных. Режим доступа для закрытых томов пулов хранения копий и томов пула активных данных обновляется до READWRITE.

Перемещение томов пула хранения копии вне площадки

После создания резервных копий первичных пулов хранения и базы данных вы можете отправить носитель с резервными копиями вне площадки. Для отправки носителей в дистанционное хранилище обозначьте тома как недоступные для IBM Spectrum Protect и отдайте носители курьеру.

Прежде чем начать

Убедитесь, что процессы резервного копирования пула хранения завершены. Это позволит избежать проблем, которые могли бы возникнуть, если бы команды **MOVE DRMEDIA** и **BACKUP STGPOOL** выполнялись одновременно.

Совет: Чтобы переместить тома хранения вне площадки, то есть, ленточные тома, содержащие данные из одного или нескольких наборов хранения, надо использовать команду **MOVE RETMEDIA** или действие **MOVE MEDIA** в Центре операций. Дополнительную информацию смотрите в разделе [“Перемещение данных набора хранения в ленточную систему хранения и из нее”](#) на стр. 71.

Процедура

1. Укажите тома с резервными копиями пула хранения копий и базы данных, которые нужно переместить вне площадки, введя команду **QUERY DRMEDIA**:

```
query drmedia * wherestate=mountable
```

2. Укажите перемещение томов, у которых текущим состоянием является MOUNTABLE, введя команду **MOVE DRMEDIA**:

```
move drmedia * wherestate=mountable
```

Для всех томов в состоянии MOUNTABLE DRM выполняет следующие задачи:

- Обновляет состояние тома на NOTMOUNTABLE и обновляет расположение тома, если вы ввели команду **SET DRMNOTMOUNTABLENAME**. Если вы не ввели эту команду, расположением по умолчанию будет NOTMOUNTABLE.
- Обновляет режим доступа к тому пула хранения копий на недоступный.
- Резервирует тома из автоматизированных библиотек.

- a) При обработке резервирования библиотеки SCSI запрашивают вмешательство оператора. Обойдите эти требования и извлеките картриджи из библиотеки, введя следующую команду:

```
move drmedia * wherestate=mountable remove=no
```

- b) Получите доступ к списку томов, которые нужно идентифицировать, и удалите картриджи из библиотеки, введя следующую команду:

```
query drmedia wherestate=notmountable
```

3. Отправьте тома в дистанционное хранилище.

4. Чтобы отслеживать тома вне площадки, введите команду **MOVE DRMEDIA**:

```
move drmedia * wherestate=notmountable
```

DRM обновит все тома в состоянии NOTMOUNTABLE до состояния COURIER, а также выполнит обновление их расположения в соответствии со значениями, заданными командой **SET DRMCOURIERNAME**. Если вы не введете команду **SET**, расположением по умолчанию будет COURIER.

Совет: Можно избежать прохождения через все состояния томов, введя команду **MOVE DRMEDIA** и задавая параметр **TOSTATE**, чтобы указать состояние назначения. Чтобы перевести тома из состояния NOTMOUNTABLE в состояние VAULT, введите следующую команду:

```
move drmedia * wherestate=notmountable tostate=vault
```

DRM обновит все тома в состоянии NOTMOUNTABLE до состояния VAULT, а также выполнит обновление их расположения в соответствии со значениями, заданными командой **SET DRMVAULTNAME**. Если команда **SET** еще не введена, то положение по умолчанию — VAULT.

5. Когда расположение хранилища подтвердит получение томов, введите команду **MOVE DRMEDIA**, чтобы указать состояние COURIER:

```
move drmedia * wherestate=courier
```

DRM обновит все тома в состоянии COURIER до состояния VAULT, а также выполнит обновление их расположения в соответствии со значениями, заданными командой **SET DRMVAULTNAME**. Если вы не введете команду **SET**, расположением по умолчанию будет VAULT.

6. Вызовите на экран список томов, содержащих действительные данные в хранилище, введя следующую команду:

```
query drmedia wherestate=vault
```

Перемещение томов пула хранения копии на площадку

Вы можете признать неvirtуальные тома резервных копий базы данных устаревшими и вернуть тома обратно на площадку для повторного использования или утилизации как часть операций по аварийному восстановлению.

Прежде чем начать

Совет: Чтобы вернуть носитель хранения на площадку, то есть тома, содержащие данные набора хранения, нужно использовать команду **MOVE RETMEDIA** или операции перемещения носителей в Центре операций. Дополнительную информацию смотрите в разделе [“Перемещение данных набора хранения в ленточную систему хранения и из нее”](#) на стр. 71.

Вы можете признать том резервной копии базы данных устаревшим, если выполняются все следующие условия:

- Возраст последнего тома набора превышает значение устаревания. Значение устаревания - это число дней после последней резервной копии в серии. При установке период устаревания равен 60 дням. Чтобы переопределить это значение, можно ввести команду **SET DRMDBBACKUPEXPIREDAYS**.
- Все тома в серии находятся в состоянии VAULT.
- Том не является частью самой последней последовательности резервных копий базы данных.

Запустите обработку устаревания вручную, введя команду **EXPIRE INVENTORY**, или автоматически, используя опцию **EXPINTERVAL**, задаваемую в файле опций сервера.

Процедура

1. Укажите срок в днях, по истечении которого серия резервных копий базы данных устареет, введя команду **SET DRMDBBACKUPEXPIREDAYS**.
Например, чтобы задать число дней, равное 30, введите следующую команду:

```
set drmdbbackupexpiredays 30
```

Совет: Введите команду **DEFINE STGPOOL** и задайте для параметра **REUSEDELAY** то же самое значение, которое находится в определении пула хранения копий, чтобы произошло следующее:

- Базу данных можно было возвратить к более раннему уровню
- Ссылки базы данных на файлы в пуле хранения копий остались действительными

Если у пулов хранения копий, которыми управляет DRM, будут разные значения **REUSEDELAY**, введите команду **SET DRMDBBACKUPEXPIREDAYS** и задайте для параметра **REUSEDELAY** самое высокое значение.

2. Укажите все тома в хранилище вне площадки, которые больше не содержат действительных данных и которые можно возвратить на площадку. Введите следующую команду **QUERY DRMEDIA** и задайте параметр **WHERESTATE=VAULTRETRIEVE**.

```
query drmedia * wherestate=vaultretrieve
```

3. Чтобы запустить процесс перемещения пула хранения копий, введите следующую команду:

```
move drmedia * wherestate=vaultretrieve
```

Ограничение: Том пула хранения копий можно переместить на площадку, если его состоянием было EMPTY хотя бы в течение числа дней, заданных параметром **REUSEDELAY** в команде **DEFINE STGPOOL**.

Сервер выполняет следующие действия для всех томов в состоянии **VAULTRETRIEVE**:

- Изменяет состояние тома на **COURIERRETRIEVE**
- Обновляет расположение тома в соответствии с тем, что задано в команде **SET DRMCOURIERNAME**

Совет:

Можно также указать пункт назначения для томов, введя команду **MOVE DRMEDIA** с параметром **TOSTATE**. Например, чтобы перевести тома из состояния **VAULTRETRIEVE** в состояние **ONSITERETRIEVE**, введите следующую команду:

```
move drmedia * wherestate=vaultretrieve tostate=onsiteretrieve
```

Сервер выполняет следующие действия для всех томов в состоянии **VAULTRETRIEVE**:

- Тома перемещаются в подключенное расположение, где их можно будет использовать повторно или утилизировать
- Тома резервной копии базы данных удаляются из таблицы хронологии томов.
- Удаляет из базы данных запись для чистых томов пула хранения копий. В случае закрытых томов пула хранения копий обновляет доступ на доступ с правом чтения и записи

4. Когда курьер возвратит тома на площадку, введите следующую команду:

```
move dimedia * wherestate=courierretrieve
```

Сервер выполняет следующие действия для всех томов в состоянии **COURIERRETRIEVE**:

- Тома перемещаются в подключенное расположение, где их можно будет использовать повторно или утилизировать
- Тома резервной копии базы данных удаляются из таблицы хронологии томов.
- Из базы данных удаляется запись для чистых томов пула хранения копий. В случае закрытых томов пула хранения копий обновляет доступ на доступ с правом чтения и записи

Перемещение данных набора хранения в ленточную систему хранения и из нее

Вы можете скопировать данные набора хранения на ленточные тома, которые можно переместить из библиотеки на площадке в хранилище лент вне площадки. Хранилища предназначены для долгосрочного защищенного хранения. После копирования набора хранения на ленту и удаления ленточного тома из ленточной библиотеки можно отслеживать перемещение тома с площадки и на площадку.

Ленточный том, содержащий данные для одного или нескольких наборов хранения, называется *томом хранения*.

По мере перемещения ленточного тома из одного места в другое состояние этого тома меняется, отражая его новое положение, и вы можете использовать эту информацию для отслеживания физического положения тома.

Жизненный цикл тома хранения состоит из следующих основных этапов:

1. Когда начинается процесс записи набора хранения на ленту, либо из пула чистых томов ленточной библиотеки выбирается чистый том, либо в пуле хранения выбирается существующий том. На этот том записываются данные из одного или нескольких наборов хранения. Когда том заполнен, курьер доставляет его в хранилище вне площадки.
2. Если том содержит данные, которые нужно восстановить, этот том извлекается из хранилища, и курьер возвращает его на площадку. После восстановления данных в наборе хранения этот том будет перемещен обратно в хранилище вне площадки.
3. Со временем срок хранения данных в наборах хранения может истечь, в зависимости от политики устаревания. Если для всех наборов хранения, данные которых есть на томе, истекут сроки хранения, том можно будет вернуть на площадку для повторного использования.

На следующем рисунке показан жизненный цикл типичной операции для перемещения томов хранения с площадки и обратно.

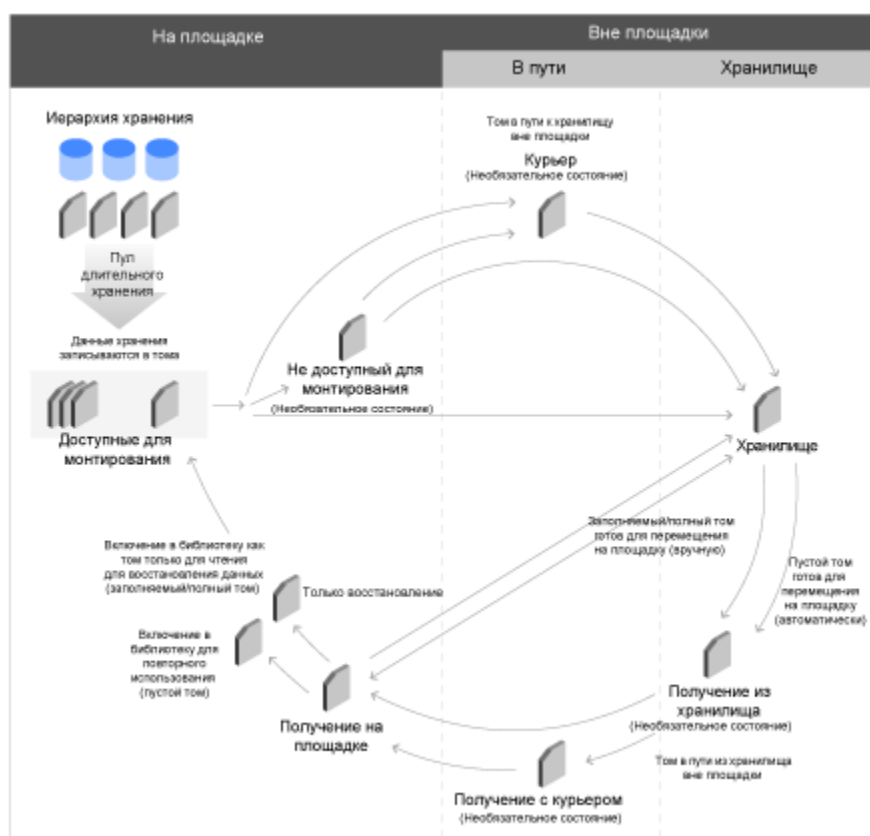


Рисунок 6. Перемещение томов хранения с площадки и на площадку

Состояние носителя тома помогает вам определить его текущее расположение, когда он перемещается из вашей библиотеки на площадку в хранилища вне площадки, а затем обратно на площадку или для восстановления данных или для повторного использования ленты. Состояние носителя тома - логическое обозначение, которое связано с физическим расположением тома. Некоторые состояния носителей необязательные. В зависимости от того, насколько хорошо ваша организация хочет отслеживать перемещения тома, ваша организация может пропустить эти необязательные состояния носителей. Показано одно из следующих состояний носителей:

MOUNTABLE

Том на площадке, и включен в библиотеку. На этот том записываются данные из одного или нескольких наборов хранения.

NOTMOUNTABLE

Том на площадке, но исключен из библиотеки и готов к отправке вне площадки.

COURIER

Том перемещается в хранилище вне площадки.

VAULT

Том помещен в хранилище вне площадки для долгосрочного хранения.

VAULTRETRIEVE

Том готов к перемещению на площадку из хранилища вне площадки. Пустые тома можно вернуть на площадку и использовать повторно. Сервер обнаруживает, что том содержит только истекшие данные и автоматически помещает том в состояние носителя VAULTRETRIEVE. Заполняющиеся или полные тома также могут быть перенесены на площадку для восстановления данных, но надо определить это действие при помощи параметра **TOSTATE** в команде **MOVE RETMEDIA**.

COURIERRETRIEVE

Том перемещается обратно на площадку из хранилища вне площадки.

ONSITERETRIEVE

Том получен из хранилища вне площадки и возвращается на площадку. Непустые тома могут быть включены в библиотеку, чтобы восстановить данные о наборе хранения из тома. Пустые тома можно включить и использовать повторно.

RESTOREONLY

Том включен в библиотеку, чтобы обеспечить восстановление данных набора хранения.

Перемещение томов хранения вне площадки

Вы можете отправлять тома хранения, содержащие данные из одного или нескольких наборов хранения вне площадки. Система хранения вне площадки предназначена для обеспечения безопасного хранения ленточных томов, а также для того, чтобы при необходимости можно было восстановить данные.

Прежде чем начать

Совет: Если вы не используете команду **MOVE DRMEDIA**, чтобы переместить тома резервного копирования базы данных, вне площадки и на площадке, можно также использовать команду **MOVE RETMEDIA**, чтобы так сделать. Дополнительную информацию смотрите в разделе [“Перемещение томов пула хранения копии вне площадки”](#) на стр. 68.

- После того, как будет создан набор хранения, который вы хотите отправить вне площадки, создайте резервные копии томов базы данных сервера, введя команду **BACKUP DB**. Если вы хотите убедиться, что том резервной копии базы данных отправлен вне площадки вместе с томом хранения, вы должны задать параметр **SOURCE** в команде **MOVE RETMEDIA**.

Ограничение: Вы не можете использовать операции перемещения носителей в Центре операций, чтобы отправить том резервной копии базы данных с площадки. Тома резервных копий базы данных перемещаются с помощью команды **MOVE RETMEDIA**.

Информацию об использовании Центра операций для перемещения томов хранения смотрите в электронной справке Центра операций.

- Убедитесь, чтобы у наборов хранения, которые вы хотите скопировать, было состояние **Завершено**. Это состояние указывает, что наборы хранения полностью копируются, чтобы записать на ленту, и ленточные тома могут быть перемещены в хранилище вне площадки. Таким образом можно избежать проблем, которые могли бы произойти, когда операции перемещения носителя и копирования наборов хранения выполняются одновременно.

Процедура

1. Укажите тома с пула длительного хранения копий и базы данных, которые нужно переместить вне площадки, введя команду **QUERY RETMEDIA**:

```
query retmedia * wherestate=mountable
```

2. Иницируйте перемещение томов, текущее состояние которых - **MOUNTABLE**. По умолчанию включаются все непустые тома, независимо от того, принадлежат ли они к наборам хранения, которые все еще копируются, или к полностью скопированным наборам хранения. Введите следующую команду:

```
move retmedia * wherestate=mountable
```

- a) Если используется библиотека SCSI, то при обработке резервирования библиотеки SCSI запрашивают вмешательство оператора. Обойдите эти требования и извлеките картриджи из библиотеки, введя следующую команду:

```
move retmedia * wherestate=mountable remove=no
```

- b) Получите список томов, которые нужно выявить и удалить из библиотеки, введя следующую команду:

```
query retmedia wherestate=notmountable
```

Для всех томов в состоянии MOUNTABLE команда **MOVE RETMEDIA** выполняет следующие задачи:

- Обновляет состояние тома на NOTMOUNTABLE и, если вы ввели команду **SET DRMNOTMOUNTABLENAME**, обновляет расположение тома. Если вы не введете команду **SET DRMNOTMOUNTABLENAME**, то положением по умолчанию будет NOTMOUNTABLE.
- Позволяет обновить режим доступа к тому.
- Резервирует тома из автоматизированных библиотек.

Совет: В зависимости от того, насколько хорошо ваша организация хочет отслеживать перемещения тома, ваша организация может пропустить некоторые состояния носителей. Можно постараться не проходить все различные состояния носителей, задав параметр **TOSTATE** в команде **MOVE RETMEDIA**, чтобы назвать целевое состояние. Например, чтобы перевести тома непосредственно из состояния NOTMOUNTABLE в состояние VAULT, введите следующую команду:

```
move retmedia * wherestate=notmountable tostate=vault
```

3. Отправьте тома курьеру для переноса вне площадки и введите следующую команду:

```
move retmedia * wherestate=notmountable
```

Все тома в состоянии NOTMOUNTABLE обновляются до состояния COURIER, а также их расположения обновляются в соответствии со значениями, заданными командой **SET DRMCOURIERNAME**. Если вы не введете команду **SET DRMCOURIERNAME**, то положением по умолчанию будет COURIER.

4. Отслеживайте перемещение ленточного тома во время его транспортировки вне площадки. Введите следующую команду:

```
query retmedia * wherestate=courier
```

5. Когда расположение хранилища подтвердит получение томов, введите команду **MOVE RETMEDIA**, чтобы указать состояние COURIER:

```
move retmedia * wherestate=courier
```

Все тома в состоянии COURIER обновляются до состояния VAULT, а также их расположения обновляются в соответствии со значениями, заданными командой **SET DRMVAULTNAME**. Если вы не введете команду **SET DRMVAULTNAME**, то положением по умолчанию будет VAULT.

Команда **MOVE RETMEDIA** обновит все тома в состоянии NOTMOUNTABLE до состояния VAULT, а также выполнит обновление их расположения в соответствии со значениями, заданными командой **SET DRMVAULTNAME**. Если команда **SET DRMVAULTNAME** еще не введена, то положение по умолчанию — VAULT.

Результаты

Тома хранения и все указанные тома резервных копий базы данных перемещаются в ленточное хранилище вне площадки. При восстановлении данных тома набора хранения можно получить из хранилища.

Перемещение томов хранения на площадке

Если нужно восстановить набор хранения, вы сможете перенести ленточные тома, содержащие данные набора хранения, на площадку для операций восстановления. Если для всех наборов хранения, у которых есть данные в томе хранения, будут достигнуты даты истечения срока хранения, вы можете использовать для повторного использования пустого тома на площадке.

Прежде чем начать

Если вы возвращаете пустые тома для повторного использования, то подтвердите, что даты истечения срока достигнуты всеми наборами хранения, у которых есть данные в томе и набор хранения истек. Можно начать обработку срока действия вручную, введя команду **EXPIRE**

INVENTORY или можно использовать команду **DELETE RESET**, чтобы пометить набор хранения для удаления.

Совет: Если вы не используете команду **MOVE DRMEDIA**, чтобы переместить тома резервного копирования базы данных, вне площадки и на площадке, можно также использовать команду **MOVE RETMEDIA**, чтобы так сделать. Дополнительную информацию смотрите в разделе [“Перемещение томов пула хранения копии вне площадки”](#) на стр. 68.

Процедура

Выполните описанные ниже шаги, чтобы переместить тома хранения на площадку.

Задача	Процедура
Переместить пустой том на площадку для повторного использования.	<p>Чтобы переместить пустые тома хранения на площадку, сделайте следующее:</p> <p>a. Найдите тома хранения в хранилище вне площадки, которые вы хотите вернуть на площадку. Для пустых томов сервер обнаруживает, что том содержит только просроченные данные, и автоматически переводит том в состояние носителя VAULTRETRIEVE. Введите следующую команду:</p> <pre>query retmedia * wherestate=vaultretrieve volstatus=empty</pre> <p>b. Переместить ленточные тома на площадку. Укажите пункт назначения для томов, введя команду MOVE RETMEDIA с параметром TOSTATE. Введите следующую команду:</p> <pre>move retmedia * wherestate=vaultretrieve volstatus=empty tostate=onsiteretrieve</pre> <p>Ограничение: Том пула длительного хранения можно переместить на площадку, если его состоянием было EMPTY хотя бы в течение числа дней, заданных параметром REUSEDELAY в команде DEFINE STGPOOL.</p> <p>Сервер выполняет следующие действия:</p> <ul style="list-style-type: none">• Изменяет состояние тома на ONSITERETRIEVE.• Тома резервной копии базы данных удаляются из таблицы хронологии томов.• Удаляет из базы данных запись для чистых томов хранения. <p>c. Включите пустой том в ленточную библиотеку и сделайте его доступным для повторного использования, введя команду CHECKIN LIBVOL и задав этот том как чистый том.</p> <p>Совет: В случае ленточных томов в библиотеках SCSI можно уменьшить время активации, указав, что сервер считывает метку штрих-кода.</p> <p>Введите следующую команду:</p> <pre>checkin libvol libname search=bulk waittime=0 checklabel=barcode status=scratch</pre>

Задача	Процедура
<p>Переместите непустой том на площадку для восстановления данных.</p>	<p>Чтобы переместить тома хранения на площадку для восстановления данных, сделайте следующее:</p> <ol style="list-style-type: none"> Укажите тома, содержащие данные набора длительного хранения, которые вы хотите восстановить. <ul style="list-style-type: none"> Чтобы определить тома, которые используются каждым набором хранения, дайте следующую команду: <pre>query retset listvolumes=yes</pre> Чтобы определить наборы хранения, у которых есть данные в томе хранения, дайте следующую команду: <pre>query volume listretsets=yes</pre> Найдите требуемый том в его положении вне площадки, введя команду QUERY RETMEDIA с параметром WHERESTATE. Например, чтобы просмотреть все тома, расположенные в хранилище вне площадки, введите следующую команду: <pre>query retmedia * wherestate=vault</pre> Переместить необходимый локальный том на площадку. Укажите пункт назначения для томов, введя команду MOVE RETMEDIA с параметром TOSTATE. Например, чтобы переместить том VOL001 на площадку, введите следующую команду: <pre>move retmedia VOL001 wherestate=vault tostate=onsiteretrieve</pre> <p>Важное замечание: Если вы возвращаете тома на площадку для восстановления данных, то оставьте пороговое значение освобождения пула хранения по умолчанию. Значение по умолчанию - 100. Таким образом, если вы перемещаете тома хранения на площадку, введя команду MOVE RETMEDIA и указав параметр TOSTATE=ONSITERETRIEVE, обработка освобождения пула хранения не будет мешать операции перемещения.</p> Включите том в ленточную библиотеку и сделайте этот том доступным для операций восстановления. Для гарантии, что том можно использовать только для восстановления данных, задается режим доступа только для чтения. Чтобы переместить том из состояния ONSITERETRIEVE в состояние RESTOREONLY, введите CHECKIN LIBVOL. Введите следующую команду: <pre>checkin libvol libname search=bulk waittime=0 checklabel=barcode status=private</pre> <p>Совет: В случае ленточных томов в библиотеках SCSI можно уменьшить время активации, указав, что сервер считывает метку штрих-кода.</p> <p>Том добавляется к автоматизированной библиотеке и состояние носителя тома изменяется на RESTOREONLY.</p>

Результаты

Выбранные тома хранения будут возвращены на площадку и помещены в ленточную библиотеку. Пустые ленточные тома возвращаются в состояние чистых томов и доступны для повторного использования. Непустые тома находятся в состоянии **RESTOREONLY** и могут использоваться, чтобы восстановить данные.

Дальнейшие действия

После того, как восстановление данных закончено, можно передать ленточные тома обратно в хранилище вне площадки. Введите следующую команду:

```
move retmedia * wherestate=restoreonly tostate=vault
```

Сообщения оповещения для отслеживания перемещения томов хранения

Если вы отправляете тома хранения с вашей площадки или возвращаете их назад, сервер IBM Spectrum Protect генерирует оповещения в виде сообщений ANR, чтобы сообщать о каких-либо проблемах и помочь вам отслеживать состояние.

Чтобы увидеть все сообщения, посмотрите журнал ошибок IBM Spectrum Protect. Подробную документацию по сообщениям смотрите в документе Сообщения ANR. Часто встречающиеся сообщения описаны в следующей таблице:

Таблица 16. Отправка ленточных томов хранения в хранилище вне площадки		
Действие	Сообщение ANR	Описание
Набор хранения скопирован на ленточный том.	ANR3852I	Это информационное сообщение указывает, что набор хранения был успешно скопирован на ленточный том. Приводятся подробности операции копирования. Состояние набора хранения - ЗАВЕРШЕН.
Ленточные тома исключены из ленточной библиотеки.	ANR6697I	Это информационное сообщение указывает, что ленточные тома в состоянии ДОСТУПЕН ДЛЯ МОНТИРОВАНИЯ были успешно изъяты из ленточной библиотеки.
Ленточный том исключен из библиотеки и перемещен из состояния ДОСТУПЕН ДЛЯ МОНТИРОВАНИЯ в состояние ХРАНИЛИЩЕ.	ANR6683I	Это информационное сообщение указывает, что данные хранения успешно перемещены и их состояние изменено.

Таблица 17. Включение ленточных томов в ленточную библиотеку для использования в описаниях восстановления		
Действие	Сообщение ANR	Описание
Том хранения, содержащий данные, был успешно включен в ленточную библиотеку лент на площадке.	ANR8532I	Это информационное сообщение указывает, что том с данными успешно включен в ленточную библиотеку на площадке. Для томов хранения состояние носителя тома изменяется с ПОЛУЧЕНИЕ НА ПЛОЩАДКЕ на ТОЛЬКО ВОССТАНОВЛЕНИЕ с режимом доступа только для чтения. Теперь данные набора хранения на этом томе доступны для восстановления. Совет: Это сообщение не появляется, если включаемый в библиотеку ленточный том пуст.
Вы пытаетесь включить в ленточную библиотеку непустой том хранения в качестве чистого тома.	ANR8443E	Это сообщение об ошибке выводится, так как том хранения, содержащий данные, нельзя включить в ленточную библиотеку с назначением состояние ЧИСТЫЙ. Этот том не включается в библиотеку, и данные на ленте не перезаписываются.

Таблица 18. Включение в ленточную библиотеку томов хранения с истекшим сроком

Действие	Сообщение ANR	Описание
Пустой том хранения включен в ленточную библиотеку на площадке.	ANR8430I	Это информационное сообщение указывает, что пустой том успешно включается в ленточную библиотеку на площадке. Этот том возвращен в состояние ЧИСТЫЙ.
Попытка включить пустой том хранения в ленточную библиотеку на площадке завершилась неудачно.	ANR8832E	Это сообщение об ошибке указывает, что операция включения пустого тома хранения в ленточную библиотеку на площадке завершилась неудачно.

Определение расписаний клиентов

Используйте Центр операций, чтобы создавать расписания для операций клиентов.

Процедура

1. В строке меню Центра операций установите указатель мыши на **Клиенты**.
2. Щелкните по **Расписания**.
3. Щелкните по **+ Расписание**.
4. Выполните шаги в мастере **Создать расписание**.

Задайте запуск расписаний резервного копирования клиента в 22:00, основываясь на операциях по обслуживанию сервера, которые вы запланировали в разделе [“Как задать расписания для операций по обслуживанию сервера”](#) на стр. 62.

Подключение ленточных устройств к серверу

Прежде чем сервер сможет использовать накопитель на магнитной ленте, надо подключить это устройство к системе сервера и установить соответствующие драйверы ленточных устройств.

Об этой задаче

Чтобы оптимизировать производительность системы, используйте быстрые ленточные устройства с высокой мощностью. Предоставьте достаточно ленточных накопителей, чтобы их число удовлетворяло вашим бизнес-требованиям.

Подключите ленточные устройства на их собственном адаптере шины хоста (host bus adapter, HBA), не используемом совместно с другими типами устройств, например, дисководом.. Ленточные накопители IBM предъявляют ряд особых требований к HBA и связанным драйверам.

Подключение устройства автоматизированной библиотеки к компьютеру

Можно подключить устройство автоматизированной библиотеки к компьютеру для сохранения данных на ленте.

Об этой задаче

Перед подключением устройства автоматизированной библиотеки ознакомьтесь со следующими ограничениями:

- Подключаемые устройства должны находиться на собственном адаптере шины хоста (Host Bus Adapter - HBA).

- Не используйте HBA совместно с другими типами устройств, такими как диски.
- В случае многопортовых адаптеров HBA Fibre Channel устройства должны подключаться к собственным портам. Эти порты не должны использоваться другими типами устройств.
- Ленточные накопители IBM имеют ряд особых требований к HBA и соответствующим драйверам. Информацию об устройствах смотрите на веб-сайте для вашей операционной системы:
 - [IBM Spectrum ProtectПоддерживаемые устройства для AIX](#)
 - [IBM Spectrum ProtectПоддерживаемые устройства для Linux и Windows](#)

Процедура

Чтобы использовать адаптер Fibre Channel (FC), сделайте следующее:

1. Установите адаптер FC и связанные драйверы.
2. Установите необходимые драйверы для подключенных устройств смены носителей.

Понятия, связанные с данным

[Выбор драйвера ленточного устройства](#)

Чтобы использовать ленточные устройства с IBM Spectrum Protect, надо установить соответствующий драйвер ленточных устройств.

Установка режима библиотеки

Чтобы обеспечить серверу IBM Spectrum Protect доступ к библиотеке SCSI, нужно задать для ленточного устройства подходящий режим.

Об этой задаче

На передних панелях некоторых библиотек предусмотрены дисплеи с меню, что дает оператору возможность формировать прямые запросы. Однако если ленточное устройство настроено на то, чтобы реагировать на такие запросы, скорее всего, оно не будет реагировать на запросы IBM Spectrum Protect.

В некоторых библиотеках предусмотрен последовательный режим (SEQUENTIAL), при котором тома автоматически последовательно монтируются на накопителях. Этот режим входит в конфликт со способом доступа IBM Spectrum Protect к ленточному устройству. Библиотека, сконфигурированная в режиме SEQUENTIAL, не обнаруживается системным драйвером устройств как устройство чейнджера библиотеки, как драйвер ленточных накопителей IBM или как драйвер ленточных устройств IBM Spectrum Protect.

Процедура

1. Чтобы узнать, как настроить режим библиотеки, смотрите документацию по вашему ленточному накопителю.
2. Установите соответствующий режим для вашего накопителя на магнитной ленте. Для большинства накопителей на магнитной ленте соответствующий режим вызывает режимом RANDOM. Если ваш накопитель на магнитной ленте не имеет режима RANDOM, найдите в документации для вашего устройства, чтобы найти соответствующий режим.

Выбор драйвера ленточного устройства

Чтобы использовать ленточные устройства с IBM Spectrum Protect, надо установить соответствующий драйвер ленточных устройств.

Ссылки, связанные с данной

[Установка и конфигурирование драйверов ленточных устройств](#)

Чтобы использовать ленточные устройства в сочетании с IBM Spectrum Protect, нужно установить соответствующий драйвер ленточных устройств.

Драйверы ленточных устройств IBM

Драйверы ленточных устройств IBM доступны для большинства маркированных устройств IBM.

Скачать драйверы ленточных устройств IBM можно с сайта Fix Central:

1. Перейдите на веб-сайт Fix Central: [Веб-сайт Fix Central](#).
2. Щелкните по **Выберите продукт**.
3. Выберите **Система хранения** в меню **Группа продуктов**.
4. Выберите **Ленточные системы** в меню **Система хранения**.
5. Выберите **Ленточные драйверы и программы** в меню **Ленточные системы**.
6. Выберите **Драйверы ленточных устройств** в меню **Ленточные драйверы и программы**. В дополнение к ленточным драйверам вы также получаете доступ к инструментам, например, инструменту диагностики IBM Tape Diagnostic Tool (ITDT).
7. Выберите свою операционную систему в меню **Платформа**.

AIX | Windows

Новейший список устройств и уровней операционных систем, поддерживаемых драйверами ленточных устройств IBM, смотрите на веб-сайте поддерживаемых устройств IBM Spectrum Protect по адресу: [Поддерживаемые устройства для AIX и Windows](#).

Linux

Новейший список ленточных устройств и уровней операционных систем, поддерживаемых драйверами ленточных устройств IBM, смотрите на веб-сайте поддерживаемых устройств IBM Spectrum Protect по адресу [Поддерживаемые устройства для Linux](#).

Драйверы ленточных устройств IBM поддерживают только некоторые уровни ядра Linux. Информацию о поддерживаемых уровнях ядра смотрите в источнике [Веб-сайт Fix Central](#).

Драйверы ленточных устройств IBM Spectrum Protect

Сервер IBM Spectrum Protect предоставляет драйверы для работы с ленточными устройствами.

Вместе с сервером устанавливается драйвер ленточных устройств IBM Spectrum Protect.

AIX

Можно использовать универсальный драйвер ленточных накопителей SCSI, обеспеченный в операционной системе IBM AIX для работы с накопителями на магнитной ленте, не поддерживаемыми драйвером устройств IBM Spectrum Protect. Если используется универсальный драйвер ленточных накопителей SCSI AIX, то класс устройства GENERICTAPE должен иметь значение типа устройства, определенный в команде **DEFINE DEVCLASS**.

В случае использования следующих ленточных устройств можно выбирать между установкой драйвера ленточных устройств IBM Spectrum Protect и собственного драйвера устройств операционной системы:

ECART

LTO (не от IBM)

Все SCSI-библиотеки, содержащие ленточные устройства из этого списка, должны использовать драйвер чейнджера IBM Spectrum Protect.

Драйверы ленточных устройств от других поставщиков оборудования могут использоваться, если они связаны с классом устройств GENERICTAPE. Универсальные драйверы устройств не поддерживаются в классах устройств WORM (write-one read-many).

Linux

Можно использовать драйвер устройств Passthru IBM Spectrum Protect. Для драйверов устройств Passthru IBM Spectrum Protect требуется универсальный драйвер устройств Linux SCSI (sg) вместе с операционной системой Linux для установки ядер.

Например, можно установить драйвер устройств Passthru IBM Spectrum Protect для следующих ленточных устройств:

ECART
LTO (не от IBM)

Все библиотеки SCSI, содержащие накопители на магнитной ленте без метки IBM из указанного списка, должны использовать драйвер устройств Passthru IBM Spectrum Protect.

Использовать универсальный драйвер устройств ленточных накопителей SCSI (st), предоставляемый операционной системой Linux, нельзя. Поэтому тип устройств GENERICTAPE не поддерживается для команды **DEFINE DEVCLASS**.

Windows Вместо драйвера устройств IBM Spectrum Protect можно выбрать собственный драйвер устройств, сертифицированный в Windows Hardware Qualification Lab. Лаборатория Windows Hardware Qualification Lab сертифицировала собственный драйвер устройств как драйвер, который можно использовать только для устройств с меткой не IBM и для ленточных накопителей не IBM. Для собственного драйвера устройства, сертифицированного лабораторией Windows Hardware Qualification Lab, можно выбрать либо драйвер устройств passthru SCSI IBM Spectrum Protect, либо собственный драйвер ленточных устройств Windows. Если используется SCSI-драйвер устройства passthru, то класс устройства в команде **DEFINE DEVCLASS** не может быть GENERICTAPE. Если используется собственный драйвер устройств, классом устройств должно быть GENERICTAPE.

Специальные имена файлов для ленточных устройств

Серверу требуется имя специального файла для ленточного устройства при работе с ленточными устройствами, сменными носителями и устройствами замены носителей.

AIX

В случае успешного конфигурирования устройства возвращается логическое имя файла. В таблице Таблица 19 на стр. 81 указано имя устройства, также называющееся имя специального файла, соответствующее накопителю или библиотеке. Для получения имени специального файла устройства можно воспользоваться командой операционной системы **SMIT**. В примерах *x* задает целое число, 0 или больше.

Таблица 19. Примеры устройств

Устройство	Пример устройства	Логическое имя файла
Ленточные накопители, поддерживаемые драйвером устройств IBM Spectrum Protect	<code>/dev/mtx</code>	<code>mtx</code>
Ленточные накопители, поддерживаемые драйвером ленточных устройств IBM	<code>/dev/rmtx</code>	<code>rmtx</code>
Ленточные накопители, поддерживаемые универсальным драйвером ленточных устройств AIX IBM	<code>/dev/rmtx</code>	<code>rmtx</code>
Устройства библиотеки, поддерживаемые драйвером устройств IBM Spectrum Protect	<code>/dev/lbx</code>	<code>lbx</code>
Устройства библиотеки, поддерживаемые драйвером ленточных устройств IBM	<code>/dev/smcx</code>	<code>smcx</code>

Linux

В случае успешного конфигурирования устройства возвращается логическое имя файла. В таблице Таблица 20 на стр. 82 указано имя устройства (другое имя - имя специального файла), соответствующее накопителю или библиотеке. В примерах *x* задает целое число, 0 или больше.

Таблица 20. Примеры устройств

Устройство	Пример устройства	Логическое имя файла
Ленточные накопители, поддерживаемые драйвером устройств Passthru IBM Spectrum Protect	<code>/dev/`tsmcs`si` /mt`x</code>	<code>mt`x</code>
Ленточные накопители, поддерживаемые драйвером устройств lin_tape IBM	<code>/dev/`IBMtape` x</code>	<code>IBMtape`x</code>
Устройства библиотеки, поддерживаемые драйвером устройств Passthru IBM Spectrum Protect	<code>/dev/`tsmcs`si` /lb`x</code>	<code>lb`x</code>
Устройства библиотеки, поддерживаемые драйвером устройств lin_tape IBM	<code>/dev/`IBMchan` ger`x</code>	<code>IBMchanger`x</code>

Windows

В случае успешного конфигурирования устройства возвращается логическое имя файла. В таблице Таблица 21 на стр. 82 указано имя устройства (другое имя - имя специального файла), соответствующее накопителю или библиотеке. В примерах *a*, *b*, *c*, *d* и *x* задают целое число, 0 или больше, где:

- *a* - ID назначения.
- *b* - LUN.
- *c* ID шины SCSI.
- *d* ID порта.

Таблица 21. Примеры устройств

Устройство	Пример устройства	Преобразованное имя устройства
Ленточные накопители, поддерживаемые драйвером устройств IBM Spectrum Protect	<code>mta.b.c.d</code>	<code>mta.b.c.d</code>
Ленточные накопители, поддерживаемые драйвером устройств Passthru IBM Spectrum Protect	<code>mta.b.c.d</code>	<code>mta.b.c.d</code>
Ленточные накопители, поддерживаемые драйвером устройств IBM	<code>Tape`x</code>	<code>mta.b.c.d</code>
Устройства библиотек, поддерживаемые драйвером устройств IBM Spectrum Protect	<code>lb.a.b.c.d</code>	<code>lba.b.c.d</code>
Устройства библиотек, поддерживаемые драйвером устройств Passthru IBM Spectrum Protect	<code>lba.b.c.d</code>	<code>lba.b.c.d</code>
Устройства библиотек, поддерживаемые драйвером устройств IBM	<code>Changer`x</code>	<code>lba.b.c.d</code>

Установка и конфигурирование драйверов ленточных устройств

Чтобы использовать ленточные устройства в сочетании с IBM Spectrum Protect, нужно установить соответствующий драйвер ленточных устройств.

IBM Spectrum Protect поддерживает все устройства, которые поддерживаются драйверами ленточных устройств IBM. Однако IBM Spectrum Protect поддерживает не все уровни операционных систем, поддерживаемые драйверами ленточных устройств IBM.

Установка и конфигурирование драйверов устройств IBM для ленточных устройств IBM

Установите и сконфигурируйте драйвер ленточных устройств IBM для использования ленточного устройства IBM.

Об этой задаче

Инструкции по установке и конфигурированию драйверов ленточных устройств IBM смотрите в разделе [Руководство по установке и использованию IBM Tape Device Drivers](#).

AIX После завершения процедуры установки в соответствии с *IBM Tape Device Drivers Installation and User's Guide* (Руководство по установке и использованию драйверов накопителей на магнитной ленте IBM) могут появиться различные сообщения, зависящие от устанавливаемого драйвера устройств. При установке драйвера для ленточного устройства IBM или библиотеки выдаются следующие сообщения:

```
rmtx Available
```

или

```
smcx Available
```

Обратите внимание на значение x, которое назначено драйвером ленточных устройств IBM. Чтобы определить имя специального файла устройства, введите одну из следующих команд:

- Для ленточных накопителей: `ls -l /dev/rmt*`
- Для ленточных библиотек: `ls -l /dev/smc*`

Имя файла может оканчиваться дополнительными символами, указывающими на различные характеристики устройств. Эти символы не требуются для IBM Spectrum Protect. Для драйверов устройств IBM в параметре **DEVICE** команды **DEFINE PATH** используется базовое имя файла для связывания устройства с накопителем (`/dev/rmtx`) или с библиотекой (`/dev/smcx`).

После установки драйвера устройства можно использовать System Management Interface Tool (SMIT), чтобы сконфигурировать ленточные накопители и ленточные библиотеки не IBM. Сделайте следующее:

1. Запустите программу интерфейса системного управления (SMIT).
2. Щелкните по **Устройства**.
3. Выберите **Устройства IBM Spectrum Protect**.
4. Выберите **Устройства, подключенные к SAN Fibre Channel**.
5. Выберите команду **Обнаружить устройства, поддерживаемые IBM Spectrum Protect**.
Дождитесь завершения процесса обнаружения.
6. Вернитесь в меню **Устройства, подключенные к SAN Fibre Channel** и щелкните по **Список атрибутов обнаруженного устройства**.

Linux После завершения процедуры установки в соответствии с *IBM Tape Device Drivers Installation and User's Guide* (Руководство по установке и использованию драйверов накопителей на магнитной ленте IBM) могут появиться различные сообщения, зависящие от устанавливаемого драйвера устройств. При установке драйвера устройств для устройства IBM LTO или 3592 будут возвращены следующие сообщения:

```
IBMtapex Available
```

или

```
IBMChangerx Available
```

Обратите внимание на значение x, которое назначено драйвером ленточных устройств IBM. Чтобы определить имя специального файла устройства, введите одну из следующих команд:

- Для ленточных накопителей: `ls -l /dev/IBMtape*`
- Для ленточных библиотек: `ls -l /dev/IBMChange*`

Имя файла может оканчиваться дополнительными символами, указывающими на различные характеристики устройств. Эти символы не требуются для IBM Spectrum Protect. Для драйверов устройств IBM в параметре **DEVICE** команды **DEFINE PATH** используется базовое имя файла для связывания устройства с накопителем (`/dev/IBMtape*`) или с библиотекой (`/dev/IBMChange*`).

Ограничение: Тип устройства этого класса не должен быть **GENERICTAPE**.

Windows В операционных системах Windows к IBM Spectrum Protect прилагается два драйвера устройств:

Драйвер устройств Passthru

Если производитель ленточного устройства предоставляет драйвер устройств SCSI, установите драйвер устройств passthru IBM Spectrum Protect.

Драйвер устройства SCSI для ленточных устройств

Если производитель ленточного устройства не предоставляет драйвер устройств SCSI, установите драйвер устройств SCSI IBM Spectrum Protect для ленточных устройств. Имя файла драйвера - `tsmscsi64.sys`.

Инструкции по установке и конфигурированию драйверов ленточных устройств IBM смотрите в публикации *IBM Tape Device Drivers Installation and User's Guide* (Руководство по установке и использованию драйверов ленточных устройств IBM). После установки драйвера ленточных устройств IBM сервер задает имя специального файла, TapeX, для ленточных устройств IBM или имя ChangeY для устройств со сменными носителями IBM. В случае драйвера устройств SCSI IBM Spectrum Protect или драйвера устройств passthru IBM Spectrum Protect можно ввести команду операционной системы Windows, **regedit**, чтобы проверять имя специального файла устройства и драйвер. На сервере IBM Spectrum Protect также есть утилита для проверки устройства для операционной системы Windows. Утилита **tsmdlst** включена в пакет сервера. Чтобы использовать утилиту, выполните следующие шаги:

1. Убедитесь, что установлен интерфейс прикладного программирования (API) адаптера шины хоста.
2. Для получения информации об устройстве из хост-системы введите:

```
tsmdlst
```

Понятия, связанные с данным

Доступ к многонаправленному вводу-выводу на ленточных устройствах IBM

Многонаправленный ввод-вывод - это метод, в котором для доступа к одному и тому же физическому устройству используются разные пути, например, через несколько адаптеров шины хоста (host bus adapter, HBA) или коммутаторов. Использование многонаправленной технологии позволяет гарантировать, что не возникнет единая точка сбоев.

Доступ к многонаправленному вводу-выводу на ленточных устройствах IBM

Многонаправленный ввод-вывод - это метод, в котором для доступа к одному и тому же физическому устройству используются разные пути, например, через несколько адаптеров шины хоста (host bus adapter, HBA) или коммутаторов. Использование многонаправленной технологии позволяет гарантировать, что не возникнет единая точка сбоев.

Драйвер ленточных устройств IBM обеспечивает поддержку многоканальности, так что если на определенном пути происходит сбой, сервер может получить доступ к устройству хранения данных по другому пути. Работающий сервер или агент хранения не обнаруживают неисправности и переходы на другой путь. Драйвер ленточных устройств IBM использует многоканальный ввод/вывод также для уравнивания динамической нагрузки, что повышает производительность операций ввода/вывода.

Для обеспечения дополнительных путей к устройствам IBM каждое устройство должно быть подключено к двум или нескольким портам на плате многопортового адаптера Fibre Channel (оптоволоконного канала) или на адаптере главной шины хоста SAS (если они доступны в

операционной системе) или к другому одному адаптеру шины хоста Fibre Channel. Если включена функция многоканального ввода/вывода и на одном из путей возникает постоянная ошибка (например, из-за неисправности HBA или кабеля), то драйверы устройств обеспечат автоматическое переключение на другой путь.

После включения функции многоканального ввода/вывода драйвер ленточных устройств IBM обнаруживает все пути к устройству на компьютере хоста. Один из путей назначается основным. Все остальные пути считаются альтернативными. Для одного устройства можно задать до 16 альтернативных путей. Для каждого пути драйвер ленточных устройств IBM создает специальный файл с уникальным именем. Прежде чем драйвер сможет создать специальный файл для пути, путь должен существовать в системе. Если путь не существует, драйвер не создаст специальный файл. Если вы воспользуетесь командой **DEFINE PATH**, чтобы задать путь для пункта назначения, укажите файл, связанный с первичным путем, в качестве значения параметра **DEVICE**.

AIX

В AIX функция многоканального ввода/вывода не включается автоматически при установке драйвера ленточных устройств IBM. Ее необходимо сконфигурировать для каждого логического устройства после установки. Многоканальный ввод/вывод остается включенным до тех пор, пока устройство не будет удалено или пока поддержка этой функции не будет отключена при конфигурировании. Инструкции по конфигурированию смотрите в публикации [Драйверы ленточных устройств IBM: Руководство по установке и использованию](#).

Для получения имен специальных файлов используется команда **ls -l**, например, **ls -l /dev/rmt***. Первичные и альтернативные пути обозначаются символами **PRI** и **ALT**, как показано в следующем примере:

```
rmt0 Available 20-60-01-PRI IBM 3590 Tape Drive and Medium Changer (FCP)
rmt1 Available 30-68-01-ALT IBM 3590 Tape Drive and Medium Changer (FCP)
```

В этом примере с ленточным накопителем IBM 3590 связаны следующие пути:

- 20-60-01-PRI
- 30-68-01-ALT

Имя специального файла, связанного с основным путем - **/dev/rmt0**. Укажите **/dev/rmt0** в качестве значения параметра **DEVICE** в команде **DEFINE PATH**.

Для просмотра подробных сведений о путях к определенному ленточному накопителю можно также использовать команду **itdt -f /dev/rmtx path**, где **x** - это число сконфигурированных ленточных накопителей. Чтобы увидеть подробные сведения о пути для определенного ленточного устройства со сменой носителей, используйте команду **itdt -f /dev/smcy path**, где **y** - это номер сконфигурированного устройства со сменой носителей.

Linux

В Linux многоканальный ввод-вывод для устройств со сменой носителей и ленточных накопителей не включается автоматически при установке драйвера устройств. Инструкции по конфигурированию многоканального ввода-вывода смотрите в публикации [Драйверы ленточных устройств IBM: Руководство по установке и использованию](#).

После включения многоканального ввода/вывода для логического устройства он остается включенным до тех пор, пока устройство не будет удалено или пока поддержка этой функции не будет отключена при конфигурировании.

Чтобы увидеть имена специальных файлов для ленточных накопителей и устройств со сменой носителей IBM, используйте команду **ls -l /dev/IBMx**, где **x** - это номер индекса устройства. Для ленточных накопителей можно также ввести команду **cat /proc/scsi/IBMtape**. Как показано в файле **IBMtape**, первичные и альтернативные пути обозначаются словами **Primary** и **Alternate**:

Number	Model	SN	HBA	FO Path
0	03592	IBM1234567	qla2xxx	Primary
1	03592	IBM1234567	qla2xxx	Alternate

Имя специального файла, связанного с основным путем для данного ленточного накопителя - /dev/IBMTape0. Укажите /dev/IBMTape0 в качестве значения параметра **DEVICE** в команде **DEFINE PATH** для данного устройства.

Для получения имен специальных файлов, связанных с основными путями ко всем устройствам смены носителей, сконфигурированным в системе, используется команда **cat /proc/scsi/IBMchanger**. Следующий пример взят из файла IBMchanger:

Number	Model	SN	HBA	FO Path
3	03584L22	IBM1002345	qla2xxx	Primary
4	03584L22	IBM1002345	qla2xxx	Alternate

Имя специального файла, связанного с основным путем для устройства смены носителей - /dev/IBMchanger3. Укажите /dev/IBMchanger3 в качестве значения параметра **DEVICE** в команде **DEFINE PATH** для данного устройства.

Чтобы увидеть подробные сведения о пути для определенного ленточного накопителя, используйте команду **itdt -f /dev/IBMTapex path**, где *x* - это номер сконфигурированного ленточного устройства. Чтобы увидеть подробные сведения о пути для определенного ленточного устройства со сменой носителей в системе, используйте команду **itdt -f /dev/IBMchangerx path**, где *x* - это номер сконфигурированного устройства со сменой носителей.

Windows В Windows многоканальный ввод-вывод для устройств со сменой носителей и ленточных накопителей не включается автоматически при установке драйвера устройств. Инструкции по конфигурированию многоканального ввода-вывода смотрите в публикации *Драйверы ленточных устройств IBM: Руководство по установке и использованию*. Если сконфигурирован многоканальный ввод-вывод, у устройства будет два совпадающих имени устройства с разными расположениями. Чтобы получить подробную информацию о первичном пути и альтернативном пути, запустите инструмент IBM Tape Diagnostic Tool с функцией **qrypath**. Выходная информация команды выглядит, как в следующем примере:

```
C:\Users\Administrator\Downloads\ITDT> .\itdt.exe qrypath -f \\.\Tape0
Запрос путей SCSI...
Всего сконфигурировано путей... 2

Альтернативный путь
Логическое устройство..... Tape0
Серийный номер..... 0000078F7612
ID хоста SCSI..... 8
Канал SCSI..... 0
ID назначения..... 3
Логическое устройство..... 0
Путь включен..... Да

Первичный путь
Логическое устройство..... Tape0
Серийный номер..... 0000078F7612
ID хоста SCSI..... 8
Канал SCSI..... 0
ID назначения..... 1
Логическое устройство..... 0
Путь включен..... Да

Завершение с кодом: 0
```

AIX Конфигурирование драйверов ленточных устройств в системах AIX

Ознакомьтесь с инструкциями, чтобы установить и сконфигурировать драйверы ленточных устройств не IBM в системах AIX.

Об этой задаче

Инструкции по установке и конфигурированию драйверов ленточных устройств IBM смотрите в публикации *Драйверы ленточных устройств IBM: Руководство по установке и использованию*.

Меню и подсказки для создания определений устройств IBM Spectrum Protect в SMIT позволяют управлять устройствами SCSI и устройствами, подключаемыми по оптоволоконным каналам (Fibre Channel, FC).

Главное меню для IBM Spectrum Protect содержит два пункта:

Устройства с интерфейсом SCSI

Этот вариант используется для конфигурирования устройств SCSI, подключенных к адаптеру SCSI на компьютере хоста.

Устройства SAN с подключением по интерфейсу fibre channel

Этот вариант используется для конфигурирования устройств, подключенных к адаптеру FC на хосте. Выберите один из следующих атрибутов:

Показать атрибуты обнаруженного устройства

Служит для вывода списка атрибутов устройства, зарегистрированного в текущей базе данных ODM.

- ID порта FC:

ID 24-битного порта FC (N(L)_порт или F(L)_порт). Это идентификатор адреса, имеющий уникальное значение в пределах сети, к которой подключено устройство. В среде с коммутатором или коммутирующей матрицей этот параметр может определяться коммутатором, при этом 2 верхних байта не равны нулю. В среде Private Arbitrated Loop в качестве значения этого параметра используется физический адрес управляемой петли (AL_PA), при этом 2 верхних байта равны нулю. Чтобы определить, каким образом назначается AL_PA или ID порта, обратитесь к производителям оборудования FC.

- Сопоставленный ID LUN:

Устройство моста FC-SCSI (которое называется также конвертером, маршрутизатором или шлюзом). Сведения о сопоставлении LUN можно получить у производителей мостов. Не следует изменять значения ID, отображенных на LUN.

- Глобальное имя (wildwide name):

Глобальное имя порта, к которому подключено устройство. Это уникальный 64-разрядный идентификатор, присваиваемый производителями компонентов FC, например, мостов, или собственных устройств FC. Обратитесь к вашим поставщикам FC, чтобы узнать глобальное имя порта.

- ID продукта:

ID продукта для устройства. Для определения идентификатора продукта обратитесь к производителям устройств.

Обнаружение устройств, поддерживаемых IBM Spectrum Protect

Эта опция служит для обнаружения устройств, поддерживаемых IBM Spectrum Protect, в сети хранения данных FC, и присвоения им состояния Доступно. При добавлении устройства в существующую среду SAN или при удалении устройства из среды необходимо повторно выполнить обнаружение устройств с помощью этой опции. Чтобы текущие значения атрибутов устройств отображались при выборе опции Список атрибутов обнаруженного устройства, необходимо сначала обнаружить устройства. Поддерживаемыми устройствами в сети хранения данных FC могут быть ленточные накопители и авточейнджеры. Драйвер устройств IBM Spectrum Protect игнорирует устройства всех других типов, например, жесткие диски.

Удаление всех определенных устройств

Эта опция служит для удаления из IBM Spectrum Protect всех устройств, подключенных к сети хранения данных FC, для которых указано состояние DEFINED в базе данных ODM. После удаления всех определенных устройств при необходимости можно повторно запустить процесс обнаружения устройств с помощью опции Обнаружить устройства, поддерживаемые IBM Spectrum Protect.

Удалить устройство

Эта опция служит для удаления из IBM Spectrum Protect одного устройства, подключенного к сети хранения данных FC, для которого указано состояние DEFINED в базе данных ODM. После удаления этого устройства при необходимости можно повторно выполнить его обнаружение с помощью опции Обнаружить устройства, поддерживаемые IBM Spectrum Protect.

AIX

Конфигурирование драйверов устройств IBM Spectrum Protect для авточейнджеров

Используйте описанную процедуру, чтобы сконфигурировать драйверы устройств IBM Spectrum Protect для авточейнджеров в библиотеках не-IBM.

Процедура

Запустите программу интерфейса системного управления (SMIT), чтобы сконфигурировать драйвер устройства для каждого авточейнджера или роботизированного устройства.

1. Выберите элемент **Устройства**.
2. Выберите элемент **IBM Spectrum ProtectУстройства**.
3. Выберите элемент **Библиотека/устройство смены носителей**.
4. Выберите команду **Добавить библиотеку/устройство смены носителей**.
5. Выберите IBM Spectrum Protect-SCSI-LB для всех библиотек, поддерживаемых IBM Spectrum Protect.
6. Выберите адаптер, к которому подключается устройство. Это число приводится в формате 00-0X, где X – это номер слота, в который установлена плата адаптера SCSI.
7. При появлении приглашения введите адрес устанавливаемого устройства для параметра CONNECTION. Адрес подключения выражается двузначным числом. Первая цифра – это идентификатор SCSI (значение, записанное в таблице). Вторая цифра – номер логического устройства SCSI (LUN), который обычно равняется нулю, если не указано иное. Идентификатор SCSI и номер LUN разделяются запятой (,).
Например, в адресе подключения 4, 0 используются идентификатор SCSI=4 и LUN=0.
8. Щелкните по **ВЫПОЛНИТЬ**.

Откроется сообщение (логическое имя файла) вида lbX Available. Запишите числовое значение X, автоматически назначаемое системой. Используйте эти сведения для заполнения поля **Имя устройства** в контрольном списке.

Например, если появится сообщение lb0 Available, то поле **Имя устройства** в контрольном списке должно содержать /dev/lb0. Всегда используйте префикс /dev/ перед именем, указанным программой SMIT.

AIX

Конфигурирование драйверов устройств IBM Spectrum Protect для ленточных накопителей

Используйте следующую процедуру для конфигурирования драйверов устройств IBM Spectrum Protect для авточейнджеров в библиотеках, приобретенных у других поставщиков.

Процедура

Важное замечание: IBM Spectrum Protect не может перезаписывать магнитные ленты *tar* или *dd*, однако программы *tar* и *dd* могут перезаписывать магнитные ленты IBM Spectrum Protect.

Ограничение: Совместное использование ленточных накопителей возможно только в случае, если накопитель не определен или сервер не запущен. Команда **MKSYSB** не действует, если IBM Spectrum Protect и AIX совместно используют один и тот же накопитель или несколько накопителей. Чтобы использовать в сочетании с устройством SCSI собственный драйвер операционной системы для ленточных устройств, устройство нужно сначала сконфигурировать в AIX, а затем в IBM Spectrum Protect. Сведения о собственных драйверах устройств смотрите в документации AIX.

Запустите программу интерфейса системного управления (SMIT), чтобы сконфигурировать драйвер устройства для каждого накопителя (в том числе для накопителей, входящих в состав библиотек).

1. Выберите элемент **Устройства**.
2. Выберите элемент **IBM Spectrum ProtectУстройства**.
3. Выберите элемент **Ленточный носитель**.
4. Выберите элемент **Добавить ленточный носитель**.
5. Выберите IBM Spectrum Protect-SCSI-MT для любого поддерживаемого ленточного накопителя.
6. Выберите адаптер, к которому подключается устройство. Это число приводится в формате 00-0X, где X - это номер слота, в который установлена плата адаптера SCSI.
7. При появлении приглашения введите адрес устанавливаемого устройства для параметра CONNECTION. Адрес подключения выражается двузначным числом. Первая цифра - это идентификатор SCSI (значение, записанное в таблице). Вторая цифра - номер логического устройства SCSI (LUN), который обычно равняется нулю, если не указано иное. Идентификатор SCSI и номер LUN разделяются запятой (,).
Например, в адресе подключения 4,0 используются идентификатор SCSI=4 и LUN=0.
8. Щелкните по **ВЫПОЛНИТЬ**. Появится сообщение:

При конфигурировании драйвера для ленточного устройства (отличного от ленточного накопителя IBM) появится сообщение (логическое имя файла) в формате `mtX Available`. Запишите числовое значение X, автоматически назначаемое системой. Используйте эти сведения для заполнения поля **Имя устройства** в контрольном списке.

Например, если появится сообщение `mt0 Available`, то поле **Имя устройства** в контрольном списке должно содержать `/dev/mt0`. Всегда используйте префикс `/dev/` перед именем, указанным программой SMIT.

AIX

Конфигурирование устройств, подключенных к SAN Fibre Channel

Чтобы сконфигурировать устройство, подключенное к SAN Fibre Channel, сделайте следующее.

Процедура

1. Запустите программу интерфейса системного управления (SMIT).
2. Выберите элемент **Устройства**.
3. Выберите элемент **IBM Spectrum ProtectУстройства**.
4. Выберите элемент **Устройства, подключенные к SAN Fibre Channel**.
5. Выберите **Обнаружить устройства, поддерживаемые IBM Spectrum Protect**. Процесс обнаружения может занять некоторое время.
6. Вернитесь в меню **Fibre Channel** и выберите **Список атрибутов обнаруженного устройства**.
7. Обратите внимание на 3-символьный идентификатор устройства, который используется при определении пути к устройству в IBM Spectrum Protect.
Например, если ленточный накопитель имеет идентификатор `mt2`, то укажите `/dev/mt2` в качестве имени устройства.

Linux

Конфигурирование драйверов ленточных устройств в системах Linux

В следующих разделах описаны установка и конфигурирование драйверов ленточных устройств в Linux.

Linux

Конфигурирование промежуточных (Passthru) драйверов IBM Spectrum Protect для ленточных накопителей и библиотек

Чтобы использовать драйвер IBM Spectrum Protect Linux Passthru, нужно выполнить описанные ниже действия.

Процедура

1. Убедитесь, что устройство подключено к системе, включено и активно.
2. Убедитесь, что устройство правильно определено системой, с помощью следующей команды:

```
cat /proc/scsi/scsi
```

3. Убедитесь, что у вас установлен пакет драйвера устройств IBM Spectrum Protect (tmscsi) и пакет сервера хранения.
4. В пакете драйвера устройств IBM Spectrum Protect существует два метода конфигурирования драйверов: `autoconf` и `tmscsi`. При использовании любого из этих способов выполняются следующие задачи.
 - Загрузка универсального драйвера SCSI операционной системы Linux (sg) в ядро.
 - Создание необходимых специальных файлов для драйвера Passthru.
 - Создание файлов сведений об устройствах для ленточных устройств (`/dev/tmscsi/mtinfo`) и библиотек (`/dev/tmscsi/lbinfo`).
5. Запустите предпочтительный для вас метод конфигурирования (`autoconf` или `tmscsi`) для драйвера IBM Spectrum Protect Passthru.

- Чтобы выполнить конфигурирование с помощью `autoconf`, введите следующую команду:

```
autoconf
```

- Чтобы осуществить конфигурирование с помощью `tmscsi`, выполните следующие действия:
 - a. Скопируйте примеры файлов конфигурации, находящиеся в каталоге установки, из `mt.conf.smp` и `lb.conf.smp` в `mt.conf` и `lb.conf`, соответственно.
 - b. Отредактируйте файлы `mt.conf` и `lb.conf`. Добавьте один раздел (как показано в примере в начале файла) для каждого сочетания конечного объекта, идентификатора и номера логического устройства SCSI. Каждое сочетание записей о конечном объекте, идентификаторе и номере логического устройства SCSI соответствует ленточному накопителю или библиотеке, которые требуется сконфигурировать. Убедитесь, что файлы соответствуют следующим требованиям.
 - Удалите пример, расположенный в начале файлов.
 - Каждый раздел должен начинаться с новой строки.
 - После последнего раздела должна начинаться новая строка.
 - Ни в одном из файлов не должно быть символа решетки (#).
 - c. Запустите сценарий `tmscsi` из каталога установки драйвера устройств.
6. Проверьте правильность конфигурирования устройства, просмотрев текстовые файлы для ленточных устройств (`/dev/tmscsi/mtinfo`) и библиотек (`/dev/tmscsi/lbinfo`).
 7. Определите имена специальных файлов для ленточных накопителей и библиотек

- Чтобы определить имена файлов для ленточных устройств, введите следующую команду:

```
> ls /dev/tmscsi/mt*
```

- Чтобы определить имена файлов для библиотек, введите следующую команду:

```
> ls /dev/tmscsi/lb*
```

Эти сведения помогают определить, какое из имен специальных файлов `/dev/tmscsi/mtx` и `/dev/tmscsi/lbx` необходимо указать для сервера при вводе команды **DEFINE PATH**.

Дальнейшие действия

При перезапуске хост-системы вы должны заново запустить сценарий `autoconf` или `tmscsi`, чтобы переконфигурировать устройства IBM Spectrum Protect. Если вы перезапустите экземпляр сервера IBM Spectrum Protect, вам не нужно переконфигурировать устройства. Как правило,

универсальный драйвер SCSI операционной системы Linux предварительно установлен в ядро. Чтобы убедиться, что драйвер загружен в ядро, введите следующую команду:

```
> lsmod | grep sg
```

Если драйвер не загружен в ядро, то введите команду **modprobe sg**, чтобы загрузить драйвер sg в ядро.

Linux Установка драйверов устройств адаптера zSeries Linux Fibre Channel (zfcp)

Драйвер устройств оптоволоконного адаптера zSeries Linux Fibre Channel (zfcp) - это специальный драйвер адаптера для системы IBM zSeries.

Об этой задаче

Драйверы ленточных устройств IBM Spectrum Protect и IBM могут работать на платформах zSeries с операционными системами Linux в 64-разрядных средах и поддерживают большую часть ленточных устройств независимых производителей оборудования (OEM) и IBM с оптоволоконными интерфейсами (Fibre Channel).

Дополнительные сведения о драйвере zfcp смотрите в публикации IBM Redpaper, *Getting Started with zSeries Fibre Channel Protocol* (Начинаем работу с протоколом zSeries Fibre Channel), которая находится по адресу: [IBM Redbooks](#).

Процедура

1. Загрузите модуль qdio.
2. Установите драйвер zfcp.
3. Отобразите протокол Fibre Channel (FCP) и сконфигурируйте драйвер zfcp.
4. Установите и сконфигурируйте драйвер ленточного устройства IBM.

Linux Информация об устройствах SCSI в системе

Информация об устройствах, которые видны вашей системе, находится в файле `/proc/scsi/scsi`. Этот файл содержит список всех обнаруженных устройств SCSI.

Представлена следующая информация об устройствах: номер хоста, номер канала, ID SCSI, номер логического устройства, поставщик, уровень программно-аппаратного обеспечения, тип устройства и режим SCSI. Например, если в системе существуют библиотеки StorageTek и IBM, шлюз SAN и несколько накопителей Quantum DLT, то файл `/proc/scsi/scsi` будет выглядеть следующим образом:

```
Attached devices:
Host: scsi2 Channel: 00 Id: 00 Lun: 00
  Vendor: STK      Model: 9738      Rev: 2003
  Type:  Medium Changer      ANSI SCSI revision: 02
Host: scsi2 Channel: 00 Id: 01 Lun: 02
  Vendor: PATHLIGHT Model: SAN Gateway Rev: 32aC
  Type:  Unknown      ANSI SCSI revision: 03
Host: scsi2 Channel: 00 Id: 01 Lun: 02
  Vendor: QUANTUM  Model: DLT7000    Rev: 2560
  Type:  Sequential-Access  ANSI SCSI revision: 02
Host: scsi2 Channel: 00 Id: 01 Lun: 04
  Vendor: IBM      Model: 7337      Rev: 1.63
  Type:  Medium Changer      ANSI SCSI revision: 02
```

Linux Предотвращение перезаписи меток магнитных лент

Драйвер устройств Passthru IBM Spectrum Protect использует универсальный драйвер устройств SCSI Linux (sg) для управления ленточными устройствами, подключенным к системе. Если универсальный драйвер ленточного устройства SCSI Linux (st) загружен в ядро и конфигурирует подключенные ленточные устройства, могут возникнуть конфликты управления устройствами, так как универсальный драйвер sg и драйвер st могут пытаться контролировать одно и то же устройство.

Об этой задаче

Если драйвер драйвер st управляет устройствами, которые использует IBM Spectrum Protect, внутренние метки лент IBM Spectrum Protect могут быть перезаписаны, и данные окажутся утерянными. Если программа использует драйвер st для управления устройствами и опция пропуска перемотки не задана, ленты автоматически перематываются после завершения операции. В ходе операции автоматической перемотки позиция ленты устанавливается в начальное положение. Если лента остается загруженной в накопитель, при следующей операции записи вне IBM Spectrum Protect метка магнитной ленты IBM Spectrum Protect перезаписывается, поскольку эта метка находится в начале ленты.

Чтобы предотвратить перезапись меток IBM Spectrum Protect, которая может привести к потере данных, убедитесь, что устройствами, используемыми IBM Spectrum Protect, управляет только драйвер Passthru IBM Spectrum Protect. Удалите драйвер st из ядра, или, если этот драйвер используют какие-либо программы в системе, удалите специальные файлы, соответствующие устройствам IBM Spectrum Protect.

Если для управления устройствами в вашей системе используется драйвер ленточных устройств IBM, то вы можете столкнуться с аналогичными проблемами при конфликте управления драйверов устройств. Посмотрите в документации к ленточным устройствам IBM, как устранить эту проблему и предотвратить потерю данных.

Удалите драйвер st

Если другие программы в системе не используют устройства st, удалите драйвер st из ядра. Чтобы выгрузить драйвер st, введите следующую команду:

```
rmmod st
```

Удалите специальные файлы, соответствующие устройствам IBM Spectrum Protect

Если существуют программы, для которых требуется использование драйвера st, можно удалить специальные файлы, соответствующие устройствам IBM Spectrum Protect. Эти специальные файлы создаются драйвером st. После удаления этих файлов драйвер st больше не сможет управлять соответствующими устройствами IBM Spectrum Protect. Специальные файлы для ленточных устройств находятся в каталоге /dev/. Формат имен: /dev/[n]st[0-1024][1][m][a].

Выведите список имен специальных файлов устройств st и список имен специальных файлов устройств IBM Spectrum Protect при помощи команды ls. На основе выведенных последовательностей устройств можно найти в списке st устройства, соответствующие устройствам в списке IBM Spectrum Protect. Удалить устройства st можно при помощи команды rm.

Введите следующие команды, чтобы вывести список устройств st и IBM Spectrum Protect:

```
ls -l /dev/*st*  
ls -l /dev/tsmcsi/mt*
```

Удалите устройства st при помощи команды rm:

```
rm /dev/*st*
```

Windows Конфигурирование драйверов ленточных устройств в системах Windows

Ознакомьтесь с инструкциями, чтобы установить и сконфигурировать драйверы для ленточных устройств и библиотек в системах Windows.

Windows Подготовка к использованию драйвера passthru IBM Spectrum Protect для ленточных устройств и библиотек

Чтобы использовать драйвер устройств passthru IBM Spectrum Protect Windows для ленточных накопителей и библиотек, надо установить драйвер и получить имена устройств, которые будет использовать сервер.

Прежде чем начать

1. Определите, предоставляет ли производитель ленточного устройства или ленточной библиотеки драйвер устройств.
2. Если производитель предоставляет пакет драйверов устройств, скачайте пакет и установите его.
3. Сконфигурируйте драйвер устройств SCSI, следуя инструкциям производителя.

Процедура

1. Установите драйвер устройств passthru IBM Spectrum Protect.
2. Получите имена устройств, которые сервер должен использовать, выполнив одно из следующих действий:
 - Введите на сервере команду **QUERY SAN**. В выходной информации будут показаны все имена устройств и связанные с ними серийные номера устройств.
 - В каталоге сервера запустите утилиту **tsmdlst.exe**. В выходной информации будут показаны все имена устройств, связанные с ними серийные номера и связанные расположения устройств.
 - В системной командной строке Windows введите команду **regedit**. Найдите в выходной информации имена файлов устройств на основе расположения устройств. Расположение состоит из ID порта, ID шины SCSI, ID LUN и ID объекта назначения SCSI. Формат имени файла устройства IBM Spectrum Protect - *mtA.B.C.D* для ленточных накопителей и *lba.B.C.D* для ленточных библиотек, где:
 - A - ID назначения SCSI.
 - B - ID LUN.
 - C - ID шины SCSI.
 - D - ID порта.

Конфигурирование драйвера SCSI IBM Spectrum Protect для ленточных устройств и библиотек

Если производитель ленточного накопителя или ленточной библиотеки не предоставляет драйвер устройств SCSI, вы должны установить драйвер устройств SCSI IBM Spectrum Protect.

Об этой задаче

Имя файла драйвера устройств SCSI IBM Spectrum Protect - `tsmscsi64.sys`.

Процедура

1. Найдите устройство на консоли менеджера устройств (`devmgmt.msc`) и выберите его. Ленточные накопители перечислены в разделе **Ленточные накопители**, а чейнджеры носителей - в разделе **Чейнджеры носителей**.
2. Сконфигурируйте устройство для использования драйвера устройств `tsmscsi64.sys`:
 - a. Щелкните правой кнопкой мыши по устройству и щелкните по **Обновить программу драйвера**.
 - b. Щелкните по **Обзор моего компьютера для поиска программы драйвера**.
3. Щелкните по **Разрешить мне выбрать из списка драйверов устройств на моем компьютере**.
4. Щелкните по **Далее**.
5. Выберите соответствующую опцию:
 - a. В случае ленточного накопителя выберите **IBM Spectrum Protect for Tape Drives**.
 - b. В случае устройства со сменой носителей выберите **IBM Spectrum Protect for Medium Changers**.
6. Щелкните по **Далее**.

7. Щелкните по **Заккрыть**.
8. Убедитесь, что устройство сконфигурировано правильно для драйвера устройств `tsmscsi64`.
 - a. Щелкните правой кнопкой мыши по устройству и щелкните по **Свойства**.
 - b. Щелкните по вкладке **Драйвер** и выберите **Сведения о драйвере**. В окне **Сведения о драйвере** будет показан драйвер устройств, управляющий устройством.

Конфигурирование библиотек для использования сервером

Чтобы использовать библиотеки для системы хранения одного сервера IBM Spectrum Protect, необходимо сначала сконфигурировать устройства в системе этого сервера.

Прежде чем начать

1. Подключите устройства к серверу. Следуйте инструкциям в разделе [“Подключение устройства автоматизированной библиотеки к компьютеру”](#) на стр. 78.
2. Выберите накопители на ленточных устройствах. Следуйте инструкциям в разделе [“Выбор драйвера ленточного устройства”](#) на стр. 79.
3. Установите и сконфигурируйте драйверы ленточных устройств. Следуйте инструкциям в разделе [“Установка и конфигурирование драйверов ленточных устройств”](#) на стр. 82.
4. Задайте имена устройств, необходимые для определения библиотеки на сервере. Следуйте инструкциям в разделе [“Специальные имена файлов для ленточных устройств”](#) на стр. 81.

Процедура

1. Задайте библиотеку и путь с сервера до библиотеки. Следуйте инструкциям в разделе [“Определение библиотек”](#) на стр. 96.
2. Определите накопители в библиотеке. Следуйте инструкциям в разделе [“Определение носителей”](#) на стр. 97.

Для библиотек SCSI можно использовать команду **PERFORM LIBACTION**, чтобы задать накопители и пути для библиотеки в один шаг, вместо выполнения двух шагов: [“2”](#) на стр. 94 и [“3”](#) на стр. 94. Чтобы использовать команду **PERFORM LIBACTION** для назначения накопителей и путей для библиотеки, нужно, чтобы поддерживалась и была включена опция **SANDISCOVERY**.

3. Задайте путь с сервера к каждому накопителю, используя команду **DEFINE PATH**.
4. Задайте класс устройств. Следуйте инструкциям в разделе [“Описание классов ленточных устройств”](#) на стр. 98.

Классы устройств задают форматы записи для накопителей и классифицируют их по типу. Используйте значение по умолчанию **FORMAT=DRIVE** как формат записи только в том случае, если все накопители, связанные с данным классом устройств, могут читать все носители и производить на них запись.

Например, у вас есть смесь накопителей Ultrium поколения 3 и Ultrium поколения 4, но у вас есть только носитель Ultrium поколения 3. Вы можете задать **FORMAT=DRIVE**, так как накопители поколения 4 и поколения 3 могут читать носители поколения 3 и производить на них запись.

5. Задайте пул хранения при помощи команды **DEFINE STGPOOL**.

Рассмотрите следующие основные варианты для определения пулов хранения:

- Чистые тома, представляющие собой пустые тома, доступные для использования. Если вы зададите максимальное число чистых томов в пуле хранения, сервер сможет выбрать тома из чистых томов, имеющихся в библиотеке.

Если использование чистых томов запрещено, необходимо выполнить дополнительные действия, чтобы явно определить каждый том, который будет использоваться в пуле хранения. Кроме этого, задайте параметр **MAXSCRATCH=0** при определении пула хранения таким образом, чтобы чистые тома не использовались.

- По умолчанию для первичных пулов хранения используется способ совместного размещения по группам. По умолчанию для пулов хранения копий и пулов активных данных совместное размещение отключено. Сервер использует *совместное размещение*, чтобы все файлы, принадлежащие группе клиентских узлов, одному клиентскому узлу, клиентскому файловому пространству или группе клиентских файловых пространств, хранились на минимальном числе томов. При отключенной функции совместного размещения для пула хранения с имеющимися в нем данными клиентов изменение данных в случае разрешения совместного размещения представляет собой непростую задачу.
6. Зарегистрируйте и пометьте тома библиотеки. Следуйте инструкциям в разделах “Регистрация томов в автоматизированной библиотеке” на стр. 191 и “Запись меток томов на ленточных томах” на стр. 189.

Убедитесь, что сервер имеет доступ к достаточному количеству томов библиотеки. Поддерживайте запас помеченных томов для предотвращения их дефицита в ходе выполнения какой-либо операции, например резервного копирования клиента. Пометьте дополнительные чистые тома для выполнения в будущем любых возможных операций восстановления.

Процедуры активации томов и присвоения им меток одинаковы для библиотек, в которых содержатся однотипные или разнотипные накопители. Команду **CHECKIN LIBVOLUME** можно использовать для регистрации томов, у которых уже есть метки. Или, при желании пометить и зарегистрировать тома за один шаг, введите команду **LABEL LIBVOLUME**.

Библиотеки с несколькими типами устройств: Если в вашей библиотеке есть накопители нескольких типов и для сервера IBM Spectrum Protect определено две библиотеки, эти две библиотеки представляют собой одну физическую библиотеку. Для каждой определенной библиотеки активация ленточных томов выполняется отдельно. Убедитесь, что тома включены в правильные библиотеки IBM Spectrum Protect.

Дальнейшие действия

Проверьте определения своих устройств и убедитесь, что все сконфигурировано правильно. Используйте команду **QUERY** для просмотра информации о каждом объекте хранения.

При проверке результатов выполнения команды **QUERY DRIVE** убедитесь, что тип устройства для накопителя соответствует ожидаемому. Если путь не задан, тип устройства накопителя будет указан как UNKNOWN, а если используется неправильный путь - будет показан GENERIC_TAPE или другой тип устройства. Этот шаг особенно важен, когда вы используете разные носители.

(Необязательно) Сконфигурируйте совместное использование библиотеки. Следуйте инструкциям в разделе “Конфигурирование совместного использования библиотеки” на стр. 105.

Информация, связанная с данной

CHECKIN LIBVOLUME (регистрация тома хранения в библиотеке)

DEFINE STGPOOL (определение тома в пуле хранения)

LABEL LIBVOLUME (запись метки на том библиотеки)

PERFORM LIBACTION (Задать или удалить все накопители и пути для библиотеки)

Определение ленточных устройств

Прежде чем вы сможете производить резервное копирование или перенос данных на ленту, вы должны задать ленточное устройство для сервера.

Определение библиотек и накопителей

В ленточной библиотеке может быть один или несколько ленточных накопителей. Узнайте, как задавать библиотеки, накопители и пути к серверу IBM Spectrum Protect.

Определение библиотек

Перед использованием накопителя следует определить библиотеку, которой он принадлежит.

Процедура

1. Задайте библиотеку, введя команду **DEFINE LIBRARY**.

Например, если у вас есть ленточная библиотека IBM TS3500, вы можете задать библиотеку ROBOTMOUNT, используя следующую команду:

```
robotmount robotmount libtype=scsi
```

Если вам требуется совместное использование библиотеки или перемещение данных в режиме без локальной сети, смотрите следующую информацию:

- “Конфигурирование совместного использования библиотеки” на стр. 105
- “Конфигурирование перемещения данных в режиме без сети;” на стр. 125

2. Задайте путь с сервера к библиотеке, используя команду **DEFINE PATH**. Задавая параметр **DEVICE**, укажите имя специального файла устройства. Это имя требуется серверу, чтобы связываться с ленточными накопителями, устройством со сменой носителей и устройствами со съемными носителями. Дополнительные сведения об именах специальных файлов устройств смотрите в разделе “Специальные имена файлов для ленточных устройств” на стр. 81.

```
AIX define path server1 robotmount srctype=server desttype=library  
device=/dev/lb0
```

```
Linux define path server1 robotmount srctype=server desttype=library  
device=/dev/tmscsi/lb0
```

```
Windows define path server1 robotmount srctype=server desttype=library  
device=lb0.0.1.0
```

Информация, связанная с данной

[DEFINE LIBRARY \(Задать библиотеку\)](#)

[DEFINE PATH \(определение пути\)](#)

Определение библиотек SCSI в сети хранения данных

Для типа библиотеки SCSI в сети хранения данных сервер может отслеживать серийный номер библиотеки. Используя серийный номер, сервер может идентифицировать устройство при указании пути или использовании устройства.

Об этой задаче

В случае необходимости можно указать серийный номер при определении библиотеки серверу. Для удобства значение по умолчанию должно позволить серверу получать серийный номер из библиотеки, когда вы задаете путь.

Если указан серийный номер, при указании пути к библиотеке сервер подтвердит правильность этого серийного номера. Задавая путь, можно ввести параметр **AUTODETECT=YES**, чтобы разрешить серверу корректировать серийный номер, если обнаруженный номер не совпадет с номером, который вы ввели, когда задавали библиотеку. Лучше всего задать параметр **AUTODETECT=YES**, чтобы автоматически обновлять серийный номер для накопителя в базе данных, когда будет создаваться определение пути.

Возможность автоматического определения сервером серийного номера зависит от функций библиотеки. Не все устройства способны вернуть серийный номер, получив запрос от такого приложения, как сервер. В этом случае сервер не запишет серийный номер устройства и не сможет подтвердить идентичность устройства при определении пути или использовании носителя сервером. Дополнительную информацию смотрите в разделе “Влияние изменений устройств в SAN” на стр. 136.

Определение носителей

Чтобы информировать сервер о диске, который может быть использован для доступа к томам хранения, выполните команду **DEFINE DRIVE**, а затем - команду **DEFINE PATH**.

Прежде чем начать

Объект накопителя представляет собой механизм в библиотеке, который использует сменный носитель. В случае устройств с несколькими накопителями, включая автоматизированные библиотеки, нужно задать каждый накопитель отдельно и связать его с библиотекой. Определения накопителей могут содержать такие сведения, как адрес элемента для накопителей в библиотеках SCSI, частота очистки ленточных накопителя и состояние подключения накопителя.

IBM Spectrum Protect поддерживает ленточные накопители, которые могут быть автономными или могут быть частью автоматизированной библиотеки. Предпочтительный метод - сконфигурировать решение на лентах с использованием автоматизированных библиотек.

Об этой задаче

При выполнении команды **DEFINE DRIVE** необходимо указать следующие данные:

Имя библиотеки

Имя библиотеки, в которой находится накопитель.

Имя носителя

Имя, назначенное накопителю.

Серийный номер

Серийный номер накопителя. Параметр серийного номера применяется только для накопителей в SCSI. Используя серийный номер, сервер может подтвердить подлинность устройства при определении пути или использовании устройства сервером.

При необходимости можно указать серийный номер. По умолчанию сервер получает серийный номер непосредственно с накопителя во время определения пути. Если указан серийный номер, при определении пути к накопителю сервер подтверждает его правильность. Задавая путь, можно задать параметр **AUTODETECT=YES**, чтобы разрешить серверу корректировать серийный номер, если обнаруженный номер не совпадет с номером, который вы ввели, когда задавали накопитель. Лучше всего задать параметр **AUTODETECT=YES**, чтобы автоматически обновлять серийный номер для накопителя в базе данных, когда будет создаваться определение пути.

В зависимости от возможностей накопителя, сервер может быть не в состоянии автоматически определить серийный номер. В этом случае сервер не запишет серийный номер устройства и не сможет подтвердить идентичность устройства при определении пути или использовании носителя сервером. Смотрите раздел [“Влияние изменений устройств в SAN”](#) на стр. 136.

Адрес элемента

Адрес элемента накопителя. Параметр **ELEMENT** применяется только для накопителей в библиотеках SCSI. Адрес элемента является числом, указывающим физическое расположение накопителя в автоматизированной библиотеке. Для связывания физического расположения накопителя и SCSI-адреса серверу требуется адрес элемента. Сервер может получить адрес элемента непосредственно с накопителя, когда вы задаете путь, либо номер элемента можно указать, когда вы будете задавать накопитель. Лучше всего задать параметр **ELEMENT=AUTODETECT**, чтобы сервер автоматически обнаруживал номер элемента, когда вы задаете путь накопителя.

Возможность автоматического определения сервером адреса элемента зависит от функций библиотеки. В данном случае, если в библиотеке содержится несколько накопителей, при определении накопителя необходимо ввести адрес элемента. Чтобы получить адрес элемента, перейдите в раздел [IBM для IBM Spectrum Protect](#).

Совет: Драйверы ленточных устройств IBM и драйверы ленточных устройств не IBM генерируют разные файлы и форматы устройств:

- В случае драйверов устройств IBM имена устройств начинаются с `imt`, после чего идет целое число, например, `/dev/imt0`.
- В случае драйверов ленточных устройств IBM Spectrum Protect имена ленточных устройств начинаются с `mt`, после чего идет целое число, например, `/dev/mt0`.

Задавая путь, нужно использовать правильный файл устройства.

Процедура

1. Назначьте накопитель в библиотеку, введя команду **DEFINE DRIVE**.
2. Чтобы сделать накопитель подходящим для использования сервером, введите команду **DEFINE PATH**.

Примеры конфигурирования библиотек, путей и накопителей смотрите в разделах [Пример: конфигурирование библиотеки SCSI или виртуальной ленточной библиотеки с одним типом накопителей](#) и [Пример: конфигурирование библиотеки SCSI или виртуальной ленточной библиотеки с несколькими типами накопителей](#).

Описание классов ленточных устройств

Класс устройства задает набор характеристик, используемых набором томов, которые можно создать в пуле хранения. Вы должны задать класс устройств для ленточного устройства, чтобы убедиться, что сервер сможет использовать устройство.

Прежде чем начать

Чтобы задать классы устройств, вначале нужно задать для сервера библиотеки и накопители.

Об этой задаче

Список поддерживаемых устройств и допустимых форматов классов устройств смотрите на веб-сайте Поддерживаемые устройства IBM Spectrum Protect для вашей операционной системы:

- [AIX](#) | [Windows](#) [Поддерживаемые устройства для AIX и Windows](#)
- [Linux](#) [Поддерживаемые устройства для Linux](#)

Для каждого типа устройств можно задать несколько классов. Например, может понадобиться указать различные атрибуты для разных пулов хранения, в которых используется один и тот же тип накопителя на магнитной ленте. Различия большей частью зависят не от самих устройств, а от того, как их планируется использовать (например, от задержек демонтирования или лимитов монтирования).

Рекомендации:

- Один класс устройств может быть связан с несколькими пулами хранения, в то время как каждый пул хранения может быть связан только с одним классом устройства.
- В SCSI-библиотеки могут входить ленточные накопители нескольких типов. При описании класса устройств в этой среде необходимо объявить значение параметра **FORMAT**.

Дополнительную информацию смотрите в разделе [“Смешанные типы устройств в библиотеке”](#) на стр. 21.

Процедура

Чтобы задать класс устройств, введите команду **DEFINE DEVCLASS** с параметром **DEVTYPE**; эта команда назначает классу устройства тип устройства.

Результаты

Если опция **DEVCONFIG** содержится в файле `dsmseiv.opt`, указанные с этой опцией файлы будут автоматически изменяться по результатам команд **DEFINE DEVCLASS**, **UPDATE DEVCLASS** и **DELETE DEVCLASS**.

Информация, связанная с данной

DEFINE DEVCLASS (Задать класс устройств)

Команда QUERY DEVCLASS (отображение информации об одном или нескольких классах устройств)

UPDATE DEVCLASS (изменение класса устройства)

Как задать классы устройств LTO

Чтобы предотвратить проблемы при одновременном использовании разных поколений накопителей LTO и носителей в одной библиотеке, смотрите ограничения. Также ознакомьтесь с ограничениями для шифрования накопителей LTO.

Использование разных поколений накопителей и устройств LTO в библиотеке

При одновременном использовании разных поколений накопителей и носителей LTO надо учитывать возможности каждого поколения с точки зрения чтения и записи. Предпочтительнее сконфигурировать разные классы устройств для каждого поколения носителей.

Об этой задаче

Если предполагается совместная работа различных поколений накопителей и носителей LTO, обратите внимание на следующие ограничения:

Таблица 22. Функции чтения-записи для накопителей LTO различных поколений									
Накопитель	Носитель 1-го поколения	Носитель 2-го поколения	Носитель 3-го поколения	Носитель 4-го поколения	Носители поколения 5	Носители поколения 6	Носители поколения 7	Носители поколения M8	Носители поколения 8
Поколение 1	Доступ чтение/запись	н/п	н/п	н/п	н/п	н/п	н/п	н/п	н/п
Поколение 2	Доступ чтение/запись	Доступ чтение/запись	н/п	н/п	н/п	н/п	н/п	н/п	н/п
Поколение 3	Доступ только для чтения	Доступ чтение/запись	Доступ чтение/запись	н/п	н/п	н/п	н/п	н/п	н/п
Поколение 4	н/п	Доступ только для чтения	Доступ чтение/запись	Доступ чтение/запись	н/п	н/п	н/п	н/п	н/п
Поколение 5	н/п	н/п	Доступ только для чтения	Доступ чтение/запись	Доступ чтение/запись	н/п	н/п	н/п	н/п
Поколение 6	н/п	н/п	н/п	Доступ только для чтения	Доступ чтение/запись	Доступ чтение/запись	н/п	н/п	н/п
Поколение 7	н/п	н/п	н/п	н/п	Права чтения	Доступ чтение/запись	Доступ чтение/запись	н/п	н/п
Поколение 8	н/п	н/п	н/п	н/п	н/п	н/п	Доступ чтение/запись	Доступ чтение/запись	Доступ чтение/запись

Пример

При совместном использовании накопителей и носителей различных типов сконфигурируйте разные классы устройств - по одному на каждый тип носителя. Чтобы задать тип носителя, используйте параметр **FORMAT** в каждом из определений классов устройств. Не указывайте FORMAT=DRIVE. Например, если используются накопители Ultrium поколения 5 и Ultrium поколения 6, задайте FORMAT=ULTRIUM5C (или ULTRIUM5) для класса устройств Ultrium поколения 5 и FORMAT=ULTRIUM6C (или ULTRIUM6) для класса устройств Ultrium поколения 6.

В этом примере оба класса устройств могут указать на одну и ту же библиотеку с накопителями Ultrium поколения 5 и Ultrium поколения 6. Накопители совместно используются между двумя пулами хранения. В одном пуле хранения используется первый класс устройства и исключительно носители Ultrium поколения 5. В другом пуле хранения используется второй класс устройства и только носители Ultrium поколения 6. Поскольку два пула хранения совместно используют одну библиотеку, носители Ultrium поколения 5 могут монтироваться в накопители Ultrium поколения 6, если они станут доступны во время обработки точки монтирования.

Если библиотека содержит и более старые поколения носителей 'только для чтения', и более новые носители 'чтение/запись', то нужно пометить носители 'только для чтения' как 'только для чтения' и зарезервировать все чистые носители 'только для чтения'. Например, если в одной библиотеке одновременно используются накопители и носители Ultrium поколений 4 и 6, то необходимо пометить носитель поколения 4 как доступный только для чтения. Кроме того, надо зарезервировать все чистые тома поколения 4.

Предельное число точек монтирования в средах со смешанными типами носителей LTO

В библиотеке со смешанными типами носителей, в которой несколько классов устройств указывают на одну библиотеку, совместимые накопители совместно используются пулами хранения. Убедитесь, что для параметра **MOUNTLIMIT** в каждом из классов устройств задано подходящее значение.

Например, в смешанной библиотеке носителей, которая содержит накопители и носители Ultrium поколений 1 и 2, носитель Ultrium поколения 1 можно смонтировать на накопителях Ultrium поколения 2.

Рассмотрим пример смешанной библиотеки, которая включает в себя следующие накопители и носители:

- Четыре накопителя LTO Ultrium поколения 1 и носители LTO Ultrium поколения 1
- Четыре накопителя LTO Ultrium поколения 2 и носители LTO Ultrium поколения 2

Вы создали следующие классы устройств:

- Класс устройств LTO Ultrium поколения 1 с именем LTO1CLASS, для которого задан параметр **FORMAT=ULTRIUM1C**
- Класс устройств LTO Ultrium поколения 2 с именем LTO2CLASS, для которого задан параметр **FORMAT=ULTRIUM2C**

Вы также создали следующие пулы хранения:

- Пул хранения LTO Ultrium поколения 1 — LTO1POOL на основе класса устройства LTO1CLASS
- Пул хранения LTO Ultrium поколения 2 — LTO2POOL на основе класса устройства LTO2CLASS

Количество точек монтирования, доступных для использования в каждом пуле хранения, указывается в классе устройства при помощи параметра **MOUNTLIMIT**. Для параметра **MOUNTLIMIT** в классе устройства LTO2CLASS должно быть установлено значение 4, соответствующее количеству доступных накопителей, в которые могут быть смонтированы только носители LTO7. Для параметра **MOUNTLIMIT** в классе устройства LTO1CLASS должно быть задано значение, превышающее число доступных накопителей (5 или, возможно, 6), чтобы скорректировать тот факт, что носители Ultrium поколения 1 могут монтироваться в накопители Ultrium поколения 2. Оптимальное значение **MOUNTLIMIT** зависит от рабочей нагрузки и шаблонов доступа к пулу хранения.

Следите за значением параметра **MOUNTLIMIT** и регулируйте его в соответствии с изменениями рабочей нагрузки. Если для параметра **MOUNTLIMIT** пула LTO1POOL установлено высокое значение, то запросы на монтирование от пула LTO2POOL могут откладываться или завершаться неудачно, поскольку накопители Ultrium поколения 2 используются для выполнения запросов на монтирование носителей Ultrium поколения 1. В наихудшем случае большое количество конфликтов накопителей Ultrium поколения 2 может вызвать ошибки монтирования носителей поколения 2, сопровождающиеся сообщением:

ANR8447E В библиотеке нет доступных накопителей.

Если для параметра **MOUNTLIMIT** пула LTO1POOL задано слишком малое значение, требования монтирования, которые могли бы быть выполнены накопителями LTO Ultrium поколения 2, будут задержаны.

Ограничение: При совместном использовании накопителей Ultrium поколения 1 и поколения 2 или 3 применяются ограничения из-за выделения точек монтирования. Например, процессы, для которых требуется несколько точек монтирования томов Ultrium поколений 1 и 2, могут пытаться зарезервировать накопители Ultrium поколения 2, даже если монтирование может быть выполнено доступным накопителем Ultrium поколения 6. Процессы, которые выполняются таким образом, включают команды **MOVE DATA** и **BACKUP STGPOOL**. Эти процессы будут ожидать, пока нужное число точек монтирования не будет получено на накопителях Ultrium поколения 2.

Информация, связанная с данной

[BACKUP STGPOOL \(резервное копирование данных основного пула хранения в пул хранения копий\)](#)

[DEFINE DEVCLASS \(Задать класс устройств\)](#)

[MOVE DATA \(Переместить файлы в том пула хранения\)](#)

Как включить и выключить шифрование накопителей для ленточных накопителей LTO поколения 4 или новее

IBM Spectrum Protect поддерживает три типа шифрования накопителей, которые доступны для накопителей LTO поколения 4 или новее: шифрование на уровне приложений, системы и библиотеки (Приложение, Система и Библиотека). Эти методы конфигурируются на аппаратном уровне.

Об этой задаче

Параметр **DRIVEENCRYPTION** в команде **DEFINE DEVCLASS** указывает, разрешено ли шифрование накопителей для форматов IBM и HP LTO поколения 4 или новее, Ultrium 4 и Ultrium 4C. Этот параметр обеспечивает совместимость IBM Spectrum Protect с настройками аппаратного шифрования пустых томов. Использовать этот параметр для заполненных или заполняющихся томов пула хранения нельзя.

IBM Spectrum Protect поддерживает метод шифрования на уровне приложений для накопителей IBM и HP LTO-4 или новее. Методы шифрования на уровне системы и библиотеки поддерживаются только накопителями IBM LTO-4 или новее. Метод шифрования на уровне библиотеки поддерживается, только если его поддерживает оборудование вашей системы (например IBM TS3500).

Ограничение: Использовать шифрование накопителей при работе с носителями с однократной записью и многократным чтением (Write-Once, Read-Many - WORM) нельзя.

Метод шифрования на уровне приложения задается на аппаратном уровне. Чтобы воспользоваться методом шифрования на уровне программы, при котором IBM Spectrum Protect создает ключи шифрования и управляет ими, задайте для параметра **DRIVEENCRYPTION** значение ON. При этом включается шифрование данных для пустых томов. Если для этого параметра задано значение ON, а в оборудовании используется другой метод шифрования, операции резервного копирования будут завершаться с ошибкой.

Процедура

Следующий упрощенный пример показывает, какие шаги нужно выполнить, чтобы включить и выключить шифрование данных на пустых томах в пуле хранения:

1. Задайте библиотеку, введя команду **DEFINE LIBRARY**:

```
define library 3584 libtype=SCSI
```

2. Задайте класс устройств LTO_ENCRYPT, введя команду **DEFINE DEVCLASS** и указав IBM Spectrum Protect в качестве менеджера ключей:

```
define devclass lto_encrypt library=3584 devtype=lto driveencryption=on
```

3. Задайте пул хранения, введя команду **DEFINE STGPPOOL**:

```
define stgpool lto_encrypt_pool lto_encrypt
```

4. Чтобы отключить шифрование новых томов, установите для параметра **DRIVEENCRYPTION** значение OFF. Значение по умолчанию - ALLOW. Шифрование пустых томов на уровне накопителя доступно, если включен другой метод шифрования.

Понятия, связанные с данным

Методы шифрования лент

Выбор используемого метода шифрования зависит от планируемого способа управления данными.

Как задать классы устройств 3592

Определения класса устройств для 3592, TS1130, TS1140, TS1150 и более поздних устройств включают параметры для ускоренного доступа к томам и шифрованием на носителях. Чтобы избежать проблем при комбинировании разных поколений накопителей 3592 и TS1130 и новее, ознакомьтесь с рекомендациями.

Использование носителей 3592 разных поколений в одной библиотеке

Для достижения оптимальной производительности не используйте носители 3592 разных поколений в одной библиотеке. При использовании разных поколений накопителей могут возникнуть ошибки носителей. Например, IBM Spectrum Protect может не прочесть метку тома.

Об этой задаче

В следующей таблице показана функциональная совместимость поколений накопителей в отношении чтения и записи.

Накопители	Формат первого поколения	Формат второго поколения	Формат третьего поколения	Формат четвертого поколения	Носители поколения 5
Поколение 1	Доступ чтение/запись	н/п	н/п	неприменимо	неприменимо
Поколение 2	Доступ чтение/запись	Доступ чтение/запись	н/п	н/п	неприменимо
Поколение 3	Доступ только для чтения	Доступ чтение/запись	Доступ чтение/запись	н/п	н/п
Поколение 4	н/п	Только для чтения	Доступ чтение/запись	Доступ чтение/запись	н/п
Поколение 5	н/п	н/п	Права чтения	Доступ чтение/запись	Доступ чтение/запись

Если вам нужно смешивать поколения накопителей в библиотеке, рассмотрите пример и ограничения, чтобы это помогло вам предотвратить проблемы.

Таблица 23. Использование накопителей разных поколений

Тип библиотеки	Пример и ограничения
SCSI	<p>Задайте новый пул хранения и класс устройств для последнего поколения носителей. Например, пусть у вас есть пул хранения и класс устройств для 3592-2. Пул хранения содержит все носители, записанные в формате поколения 2. Предположим, что в определении класса устройств для параметра FORMAT задано значение 3952-2 (не FORMAT). Вы добавляете в библиотеку накопители поколения 3. Сделайте следующее:</p> <ol style="list-style-type: none"> 1. В новом определении класса устройств для накопителей поколения 3 задайте для параметра FORMAT значение 3592-3 или 3592-3C. Не задавайте значение DRIVE. 2. В определении пула хранения, связанного с накопителями поколения 2, обновите параметр MAXSCRATCH до 0, например: <pre>update stgpool genpool2 maxscratch=0</pre> <p>При таком методе оба поколения смогут использовать оптимальный для себя формат, и можно будет свести к минимуму потенциальные ошибки носителей, связанные с использованием разных поколений. Однако он не разрешает всех проблем с носителями. Например, возможны конфликты точек монтирования и ошибки монтирования. (Чтобы подробнее узнать о конкуренции точек монтирования в контексте накопителей 3592 и носителей, смотрите раздел “Как задать классы устройств 3592” на стр. 102.)</p> <p>Ограничение: Ниже описаны ограничения, действующие в отношении носителей:</p> <ul style="list-style-type: none"> • CHECKIN LIBVOL: При использовании опции CHECKLABEL=YES существует неразрешенная проблема. Если метка записывается в формате поколения 3 или новее и вы зададите опцию CHECKLABEL=YES, накопители предыдущих поколений не будут работать при использовании этой команды. Во избежание проблем задайте CHECKLABEL=BARCODE. • LABEL LIBVOL: Когда сервер пытается использовать накопители предыдущего поколения для чтения метки, записанной в формате поколения 3 или новее, команда LABEL LIBVOL завершится неудачно, если не задан параметр OVERWRITE=YES. Убедитесь, что на носителе, для которого указано OVERWRITE=YES, нет никаких активных данных. • CHECKOUT LIBVOL: Когда IBM Spectrum Protect проверяет метку (CHECKLABEL=YES) как формат поколения 3 или новее и читает накопители предыдущих поколений, команда завершается неудачно. Во избежание этой проблемы задайте CHECKLABEL=NO.

Информация, связанная с данной

[CHECKIN LIBVOLUME](#) (регистрация тома хранения в библиотеке)

[CHECKOUT LIBVOLUME](#) (исключение тома хранения из библиотеки)

[LABEL LIBVOLUME](#) (запись метки на том библиотеки)

[UPDATE STGPOOL](#) (обновить пул хранения)

Управление скоростью доступа к данным для томов в классе устройств 3592

При создании томов можно оптимизировать емкость хранения и повысить скорость доступа к данным. Разбивая данные на пулы хранения, в которых есть тома, вы можете задать процент масштабируемой емкости, чтобы обеспечить максимальную емкость хранения или быстрый доступ к тому.

Об этой задаче

Чтобы уменьшить емкость носителей, задайте параметр **SCALECAPACITY**, когда будете задавать класс устройств с использованием команды **DEFINE DEVCLASS** или когда будете обновлять класс устройств с использованием команды **UPDATE DEVCLASS**.

Задайте значение в процентах, равное 20, 90 или 100. Значение, равное 20 процентам, обеспечит самый быстрый доступ к данным, а 100 процентам - самую большую емкость для хранения данных. Например, если вы укажете масштабирование емкости, составляющее 20%, для класса устройств 3592 (без сжатия), емкость тома формата 3592 в устройстве этого класса будет составлять 20% от полной емкости, равное 300 ГБ (около 60 ГБ).

Масштабирование емкости действует только при первой записи данных на том. Никакие изменения класса устройств с целью масштабирования емкости не повлияют на тома, если на них уже записаны данные, пока том не будет переведен в чистое состояние.

Информация, связанная с данной

[DEFINE DEVCLASS \(Задать класс устройств\)](#)

[UPDATE DEVCLASS \(изменение класса устройства\)](#)

Как включить и выключить шифрование накопителей 3592 поколения 2 и новее

При работе с IBM Spectrum Protect можно использовать следующие типы шифрования накопителей для накопителей 3592 второго и последующих поколений: шифрование на уровне программ, системы и библиотеки. Эти методы конфигурируются на аппаратном уровне.

Об этой задаче

Параметр **DRIVEENCRYPTION** в команде **DEFINE DEVCLASS** указывает, разрешено ли шифрование накопителей для накопителей 3592 поколения 2 и новее. Используйте этот параметр для обеспечения совместимости IBM Spectrum Protect с настройками аппаратного шифрования пустых томов. Использовать этот параметр для заполненных или заполняющихся томов пула хранения нельзя.

- Чтобы воспользоваться методом шифрования на уровне программы, при котором IBM Spectrum Protect создает ключи шифрования и управляет ими, задайте для параметра **DRIVEENCRYPTION** значение **ON**. Это позволяет шифровать данные на пустых томах. Если для параметра задано значение **ON**, а устройство сконфигурировано для использования другого метода шифрования, операции резервного копирования будут завершаться неудачно.
- Чтобы использовать методы шифрования на уровне библиотеки или системы, установите для параметра значение **ALLOW**. Таким образом, IBM Spectrum Protect не будет управлять шифрованием накопителей, но даст возможность оборудованию шифровать данные на томе одним из других методов. Указание этого параметра не означает автоматического шифрования дисков. Данные могут шифроваться только путем указания параметра **ALLOW** и конфигурирования оборудования на один из этих методов.

Параметр **DRIVEENCRYPTION** является необязательным. Значение по умолчанию позволяет использовать методы шифрования на уровне библиотеки или системы.

Процедура

В приведенном ниже упрощенном примере показано, как, используя IBM Spectrum Protect в качестве менеджера ключей, зашифровать данные на пустых томах в пуле хранения:

1. Задайте библиотеку, введя команду **DEFINE LIBRARY**.

Например, введите следующую команду:

```
define library 3584 libtype=SCSI
```

2. Задайте класс устройств, 3592_ENCRYPT, введя команду **DEFINE DEVCLASS** и задав значение **ON** для параметра **DRIVEENCRYPTION**.

Например, введите следующую команду:

```
define devclass 3592_encrypt library=3584 devtype=3592 driveencryption=on
```

3. Задайте пул хранения.

Например, введите следующую команду:

```
define stgpool 3592_encrypt_pool 3592_encrypt
```

Дальнейшие действия

Чтобы отключить все методы шифрования новых томов, установите для параметра **DRIVEENCRYPTION** значение OFF. Если оборудование сконфигурировано на шифрование данных на уровне библиотеки или системы, а для параметра **DRIVEENCRYPTION** установлено значение OFF, операции резервного копирования данных будут завершаться с ошибкой.

Конфигурирование совместного использования библиотеки

Несколько серверов IBM Spectrum Protect могут совместно использовать устройства хранения при помощи сети хранения данных. Вы настраиваете один сервер как менеджера библиотеки, а другие серверы - как клиентов библиотеки.

Прежде чем начать

Убедитесь, что ваши системы соответствуют требованиям лицензирования для совместного использования библиотек. Для каждого сервера IBM Spectrum Protect, сконфигурированного в качестве клиента библиотеки или менеджера библиотеки в среде SAN, требуется предоставленное право на IBM Spectrum Protect for SAN.

Об этой задаче

При перемещении данных в режиме без локальной сети клиентские системы IBM Spectrum Protect могут непосредственно обратиться к устройствам хранения, определенным для сервера IBM Spectrum Protect. Для выполнения перемещения данных агенты хранения устанавливаются и конфигурируются в клиентских системах.

Чтобы сконфигурировать совместное использование библиотеки, необходимо определить один сервер IBM Spectrum Protect как менеджер библиотеки для вашей конфигурации библиотеки совместного использования. Затем вы задаете другие серверы IBM Spectrum Protect как клиенты библиотеки, связывающиеся с менеджером библиотеки и запрашивающие у него ресурсы хранения. Сервер менеджера библиотеки должен быть той же версии или новее, чем сервер или серверы, определенные как клиенты библиотеки.

Процедура

Чтобы обеспечить совместное использование ресурсов библиотеки в SAN на серверах IBM Spectrum Protect, выполните следующие шаги:

1. Установить связь между серверами.

Чтобы совместно использовать устройство хранения в сети хранения данных (SAN), определите серверы друг для друга при помощи функции перекрестного определения. У каждого сервера должно быть уникальное имя.

2. Задайте библиотеку совместного использования и сконфигурируйте ленточные устройства в системах серверов.

Используйте процедуру, описанную в разделе [“Конфигурирование библиотек для использования сервером”](#) на стр. 94, чтобы определить библиотеку для среды совместного использования. Измените процедуру для определения библиотеки как совместно используемой, задав параметр **SHARED=YES** для команды **DEFINE LIBRARY**.

3. Определите сервер менеджера библиотеки.

4. Задайте совместно используемую библиотеку на сервере, который является клиентом библиотеки.

5. На сервере менеджера библиотеки определите пути от клиента библиотеки к каждому носителю, доступному для клиента библиотеки.

Имя устройства должно отражать способ, по которому система клиента библиотеки распознает это ленточное устройство. Пути от менеджера библиотеки к каждому ленточному накопителю должны определяться в том порядке, в каком клиент библиотеки будет использовать эти накопители.

Чтобы избежать проблем убедитесь, что все пути накопителей, заданные для менеджера библиотеки, также заданы для каждого клиента библиотеки.

Например, если в менеджере библиотеки заданы три ленточных накопителя, на клиенте библиотеки также должны быть заданы три ленточных накопителя. Чтобы ограничить число накопителей, которые клиент библиотеки может использовать одновременно, используйте параметр **MOUNTLIMIT** для класса устройств на клиенте библиотеки.

6. Определите классы устройств для совместно используемой библиотеки.

Рекомендуется задавать одинаковые имена классов устройств на обоих серверах, чтобы исключить путаницу при определении нескольких классов устройств одного типа с одинаковыми параметрами библиотеки. Некоторые операции, такие как резервное копирование базы данных, используют имя класса устройства для идентификации данных для резервного копирования.

Параметры класса устройств, заданные в менеджере библиотеки, переопределяют параметры, заданные для клиента библиотеки. Если имена классов устройств различаются, менеджер библиотеки использует параметры, указанные в классе устройства, который соответствует типу устройства, указанному для клиента библиотеки.

7. Определите пул хранения для совместно используемой библиотеки.

8. Повторите эти шаги, чтобы сконфигурировать другой сервер в качестве клиента библиотеки.

Информация, связанная с данной

[DEFINE DEVCLASS \(Задать класс устройств\)](#)

[DEFINE LIBRARY \(Задать библиотеку\)](#)

[DEFINE STGPOOL \(определение тома в пуле хранения\)](#)

Linux | AIX **Пример: совместное использование библиотек для серверов AIX и Linux**

Чтобы узнать, как настроить среду совместного использования библиотек SCSI для серверов, работающих в системах AIX или Linux, смотрите пример процедуры.

Об этой задаче

В этом примере конфигурируется сервер менеджера библиотеки с именем ASTRO и клиент библиотеки с именем JUDY. Для подсказки, где какой шаг используется, командам предшествует имя сервера, на котором их нужно вводить. Большинство команд вводится в клиенте библиотеки.

Для библиотек SCSI задайте библиотеку, указав параметр **libtype=scsi**.

Процедура

1. Чтобы сконфигурировать ASTRO как сервер менеджера библиотеки, определите библиотеку совместного использования SCSI с именем SANGROUP.

Например:

```
astro> define library sangroup libtype=scsi shared=yes
```

Затем выполните остальные шаги, как описано в разделе [Пример: конфигурирование библиотеки SCSI или виртуальной ленточной библиотеки с одним типом накопителей](#), чтобы сконфигурировать библиотеку.

Совет: Команду **PERFORM LIBACTION** можно использовать для определения накопителей и нутей для библиотеки в один шаг.

2. Определите ASTRO как сервер менеджера библиотеки, введя команду **DEFINE SERVER**.

```
judy> define server astro serverpassword=secret hladdress=192.0.2.24  
lladdress=1777 crossdefine=yes
```

3. Определите библиотеку совместного использования SANGROUP, введя команду **DEFINE LIBRARY**. Необходимо использовать имя сервера менеджера библиотеки в параметре **PRIMARYLIBMANAGER** и равенство **LIBTYPE=SHARED**.

```
judy> define library sangroup libtype=shared primarylibmanager=astro
```

Убедитесь, что имя библиотеки совпадает с именем библиотеки, указанным в менеджере библиотеки.

4. Определите пути от менеджера библиотеки ASTRO к двум накопителям в библиотеке совместного использования, введя команду **DEFINE PATH**.

```
AIX astro> define path judy drivea srctype=server desttype=drive  
library=sangroup device=/dev/rmt6  
astro> define path judy driveb srctype=server desttype=drive  
library=sangroup device=/dev/rmt7
```

```
Linux astro> define path judy drivea srctype=server desttype=drive  
library=sangroup device=/dev/IBMtape6  
astro> define path judy driveb srctype=server desttype=drive  
library=sangroup device=/dev/IBMtape7
```

5. Определите все классы устройств, связанные с данной совместно используемой библиотекой.

```
AIX judy> define devclass tape library=sangroup devtype=lto
```

```
Linux judy> define devclass tape library=sangroup devtype=lto
```

Следующие параметры определения класса устройств должны быть одинаковы для клиента библиотеки и для менеджера библиотеки:

- **LIBRARY**
- **DRIVEENCRYPTION**
- **WORM**
- **FORMAT**

6. Определите пул хранения с именем BACKTAPE для библиотеки совместного использования, которая будет использоваться. Введите команду **DEFINE STGPOOL**.

```
judy> define stgpool backtape tape maxscratch=50
```

Дальнейшие действия

Повторите эту процедуру для определения других клиентов библиотеки для вашего менеджера библиотеки.

Информация, связанная с данной

[DEFINE DEVCLASS \(Задать класс устройств\)](#)

[DEFINE DRIVE \(Задать накопитель для библиотеки\)](#)

[DEFINE LIBRARY \(Задать библиотеку\)](#)

[DEFINE PATH \(определение пути\)](#)

[DEFINE STGPOOL \(определение тома в пуле хранения\)](#)

Пример: совместное использование библиотек для серверов Windows

Чтобы узнать, как настроить среду совместного использования библиотек для серверов, работающих в системах Windows, ознакомьтесь с примером процедуры.

Об этой задаче

В этом примере конфигурируется сервер менеджера библиотеки с именем ASTRO и клиент библиотеки с именем JUDY.

Для библиотек SCSI задайте библиотеку, указав параметр **libtype=scsi**.

Настройка сервера менеджера библиотеки

Вы должны настроить сервер менеджера библиотеки, чтобы сконфигурировать серверы IBM Spectrum Protect для совместного использования устройств, подключенных к SAN.

Процедура

Следующая процедура - это пример того, как задать сервер IBM Spectrum Protect с именем ASTRO в качестве менеджера библиотек:

1. Убедитесь, что сервер менеджера библиотек работает:
 - a) Запустите консоль управления службами Windows (services.msc).
 - b) Выберите службу. Например, TSM Server1.
 - c) Если служба не работает, то щелкните правой кнопкой мыши по имени службы и щелкните по **Пуск**.
2. Получите информацию о библиотеке и драйвере для устройства совместно используемой библиотеки:
 - a) Запустите файл tsmdlst.exe. Эта утилита находится в каталоге \Program Files\Tivoli\TSM\server.
3. Задайте тип библиотеки SCSI.
Например:

```
define library sangroup libtype=scsi shared=yes
```

В данном примере используется стандартный серийный номер библиотеки, то есть сервер получает номер из самой библиотеки при определении пути. Возможность автоматического определения сервером серийного номера зависит от функций библиотеки. В этом случае сервер не запишет серийный номер устройства и не сможет подтвердить идентичность устройства при определении пути или использовании носителя сервером.

4. Задайте для сервера путь к библиотеке:

```
define path astro sangroup srctype=server desttype=library  
device=lb0.0.0.2
```

Если при определении библиотеки не указан серийный номер, сервер отправит запрос библиотеке, чтобы получить эти данные. Если при определении библиотеки был указан серийный номер, сервер проверит указанную информацию и в случае несовпадения выведет соответствующее сообщение.

5. Определите накопители в библиотеке.

```
define drive sangroup drivea  
define drive sangroup driveb
```

В данном примере используется стандартная процедура получения серийного номера накопителя, то есть сервер получает серийный номер из самой библиотеки во время определения пути. В зависимости от возможностей накопителя, сервер может быть не в состоянии автоматически определить серийный номер. В этом случае сервер не запишет серийный номер устройства и не сможет подтвердить идентичность устройства при определении пути или использовании носителя сервером.

В данном примере также используется стандартный адрес элемента накопителя, который сервер получает непосредственно с диска во время определения пути.

Адрес элемента является числом, указывающим физическое расположение накопителя в автоматизированной библиотеке. Для связывания физического расположения накопителя и SCSI-адреса серверу требуется адрес элемента. Сервер может получить номер элемента непосредственно с носителя во время определения пути, или его можно указать при определении носителя.

Возможность автоматического определения сервером адреса элемента зависит от функций библиотеки. В этом случае при определении носителя нужно ввести адрес элемента. Номера элементов для многих библиотек можно найти на сайте [IBM для IBM Spectrum Protect](#).

6. Задайте путь от сервера к каждому диску.

```
define path astro drivea srctype=server desttype=drive library=sangroup
device=mt0.1.0.2
define path astro driveb srctype=server desttype=drive library=sangroup
device=mt0.2.0.2
```

Если при определении накопителя не был указан серийный номер или адрес элемента, сервер направит запрос библиотеке, чтобы получить эти данные.

7. Задайте хотя бы один класс устройств.

```
define devclass tape devtype=dlt library=sangroup
```

8. Добавить в перечень библиотеки. В следующем примере выполняется регистрация всех томов в перечне библиотеки в качестве чистых томов. Сервер использует имя на метке штрих-кода в качестве имени тома.

```
checkin libvolume sangroup search=yes status=scratch
checklabel=barcode
```

9. Настройте пул хранения для совместно используемой библиотеки, содержащей не более 50 чистых томов.

```
define stgpool backtape tape
description='storage pool for shared sangroup' maxscratch=50
```

Информация, связанная с данной

[CHECKIN LIBVOLUME \(регистрация тома хранения в библиотеке\)](#)

[DEFINE DEVCLASS \(Задать класс устройств\)](#)

[DEFINE DRIVE \(Задать накопитель для библиотеки\)](#)

[DEFINE LIBRARY \(Задать библиотеку\)](#)

[DEFINE PATH \(определение пути\)](#)

[DEFINE STGPOOL \(определение тома в пуле хранения\)](#)

Windows Установка серверов клиентов библиотеки

Нужно настроить один или несколько серверов клиента библиотеки, чтобы сконфигурировать серверы IBM Spectrum Protect для совместного использования устройств, подключенных к SAN.

Прежде чем начать

Убедитесь, что сервер менеджера библиотек задан.

Об этой задаче

Нужно задать сервер менеджера библиотеки. Ниже приведен пример процедуры настройки сервера IBM Spectrum Protect с именем JUDY в качестве клиента библиотеки.

Процедура

1. Убедитесь, что сервер менеджера библиотек работает:
 - a) Запустите консоль управления службами Windows (services.msc).
 - b) Выберите службу. Например, TSM Server1.
 - c) Если служба не работает, то щелкните правой кнопкой мыши по имени службы и выберите **Пуск**.
2. Получите информацию о библиотеке и драйвере для устройства совместно используемой библиотеки:
 - a) Запустите файл tsmdlst.exe. Эта утилита находится в каталоге \Program Files\Tivoli\TSM\server.
3. Задайте совместно используемую библиотеку, SANGROUP, и укажите менеджер библиотеки. Убедитесь, что имя библиотеки совпадает с именем библиотеки, указанным в менеджере библиотеки.

```
define library sangroup libtype=shared primarylibmanager=astro
```

4. Задайте пути от сервера клиента библиотеки до каждого из накопителей, введя команды на административном клиенте:

```
define path judy drivea srctype=server desttype=drive library=sangroup  
device=mt0.1.0.3  
define path judy driveb srctype=server desttype=drive library=sangroup  
device=mt0.2.0.3
```

5. Задайте хотя бы один класс устройств, введя команды с клиента библиотеки:

```
define devclass tape devtype=dlt mountretention=1 mountwait=10  
library=sangroup
```

Параметры класса устройства для клиента библиотеки задайте равными параметрам, установленным для менеджера библиотеки. Задание одинаковых имен классов устройств на обоих серверах рекомендуется, но не является обязательным.

Параметры класса устройств, заданные на сервере менеджера библиотек переопределяют параметры, заданные для клиента библиотеки. Это правило действует независимо от того, имеют ли классы устройств одинаковые имена на обоих серверах. Если имена классов устройств различаются, менеджер библиотеки использует параметры, указанные в классе устройства, совпадающем с типом устройства, заданным для клиента библиотеки.

Если необходимо, чтобы какой-либо параметр клиента библиотеки имел значение, отличающееся от значения параметра класса устройства менеджера библиотеки (например, лимит монтирования), то сделайте следующее:

- a. Создайте дополнительный класс устройства на сервере менеджера библиотеки. Укажите нужные значения параметров для клиента библиотеки.
 - b. Создайте класс устройства на клиенте библиотеки с таким же именем и типом устройства, как у нового класса устройства, созданного на сервере библиотеки.
6. Задайте пул хранения (BACKTAPE) для совместно используемой библиотеки:

```
define stgpool backtape tape  
description='storage pool for shared sangroup' maxscratch=50
```

7. Повторите эту операцию, чтобы задать дополнительные сервера как клиенты библиотеки.

Информация, связанная с данной

[DEFINE DEVCLASS \(Задать класс устройств\)](#)

[DEFINE LIBRARY \(Задать библиотеку\)](#)

[DEFINE PATH \(определение пути\)](#)

[DEFINE STGPOOL \(определение тома в пуле хранения\)](#)

Настройка иерархии пулов хранения

В ходе процесса реализации вы должны настроить иерархию пулов хранения. Настройте хотя бы один первичный пул хранения на диске и один первичный пул хранения на ленте. Убедитесь, что ежедневно осуществляется перенос данных с диска на ленту.

Прежде чем начать

1. Убедитесь, что вы ознакомились с информацией в [“Планирование иерархии пулов хранения”](#) на стр. 23.
2. Убедитесь, что для резервного копирования данных клиента заданы соответствующие правила, которые также называются *политикой*. Следуйте инструкциям в разделе [“Как задать роли для резервного копирования и архивирования данных клиента”](#) на стр. 115.
3. Убедитесь, что политика назначена для каждого узла. Инструкций по назначению политики при регистрации узла смотрите в разделе [“Регистрация клиентов”](#) на стр. 120.

Процедура

Чтобы настроить иерархию пулов хранения, выполните следующие шаги:

1. Задайте первичный пул хранения для ленточного устройства, введя команду **DEFINE STGPOOL**.

Например, задайте первичный пул хранения TAPE1 с классом устройств LTO и включите совместное размещение группы. Задайте максимальное число чистых томов, которые сервер может потребовать для данного пула хранения, равное 999. Введите следующую команду:

```
define stgpool tape1 lto pooltype=primary collocate=group  
maxscratch=999
```

2. Задайте накопители, пути и библиотеки для первичного пула хранения на ленте. Следуйте инструкциям в разделе [“Определение ленточных устройств”](#) на стр. 95.
3. Задайте первичный пул хранения для дискового устройства, введя команду **DEFINE STGPOOL**.

Например, задайте пул хранения DISK1 с классом устройств FILE. Убедитесь, что данные можно переносить в ленточный пул хранения, TAPE1, но запретите автоматический перенос, задав значение 100 для параметра **HIGHMIG** и значение 0 для параметра **LOWMIG**. Запретите освобождение пространства, задав значение 100 для параметра **RECLAIM**. Включите совместное размещение для узлов. Задайте максимальное число чистых томов, которые сервер может потребовать для данного пула хранения, равное 9999. Используйте параметр **MIGPROCESS**, чтобы задать число процессов переноса. Значение параметра **MIGPROCESS** должно равняться числу накопителей в библиотеке минус число накопителей, зарезервированных для операций восстановления. Введите следующую команду:

```
define stgpool disk1 file pooltype=primary nextstgpool=tape1  
highmig=100 lowmig=0 reclaim=100 collocate=node maxscratch=9999 migprocess=5
```

Дополнительную информацию о том, как настроить перенос с диска на ленту, смотрите в разделе [Перенос дисковых пулов хранения](#).

Дальнейшие действия

Иерархия пула хранения содержит только первичные пулы хранения. После настройки иерархии пулов хранения выполните следующие шаги:

1. Создайте пул хранения копий на ленточном устройстве. Инструкции смотрите в разделе [DEFINE STGPOOL \(определение пула хранения копий, которому назначены устройства с последовательным доступом\)](#).

2. Создайте резервную копию первичного пула хранения на основе лент в пуле хранения копий, используя команду **BACKUP STGPOOL**. Инструкции смотрите в разделе [BACKUP STGPOOL](#) (резервное копирование данных основного пула хранения в пул хранения копий).
3. Чтобы убедиться, что можно будет восстановить данные после аварии, настройте процедуру перемещения ленточных томов из пула хранения копий в расположение вне площадки. Инструкции смотрите в разделе [“Подготовка к аварии и восстановление после аварии с использованием DRM”](#) на стр. 225.

Информация, связанная с данной

[CHECKIN LIBVOLUME](#) (регистрация тома хранения в библиотеке)

[DEFINE STGPOOL](#) (определение тома в пуле хранения)

Защита приложений и компьютеров

Сервер защищает данные для клиентов, которые могут включать в себя приложения, виртуальные машины и системы.

Добавление клиентов

После успешной настройки сервера IBM Spectrum Protect установите и сконфигурируйте программу клиента, чтобы начать резервное копирование данных.

Об этой задаче

Процедура описывает базовые шаги по добавлению клиента. Более конкретные инструкции по конфигурированию клиентов смотрите в документации по продукту, который вы установили на клиентском узле. У вас могут быть следующие типы клиентских узлов:

Клиентские узлы приложений

К клиентским узлам приложений относятся серверы электронной почты, базы данных и другие приложения. Например, клиентским узлом приложения может быть любое из следующих приложений:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

Системные клиентские узлы

К системным клиентским узлам относятся рабочие станции, файл-серверы сетевой системы хранения данных (NAS) и клиенты API.

Клиентские узлы виртуальных машин

Клиентские узлы виртуальных машин представляют собой отдельные хосты-гости в гипервизоре. Каждая виртуальная машина представлена как файловое пространство.

Процедура

Чтобы добавить клиент, сделайте следующее:

1. Выберите программу, которую нужно установить на клиентском узле, и спланируйте установку. Следуйте инструкциям в разделе [“Выбор программного обеспечения клиента и планирование установки”](#) на стр. 113.
2. Укажите, как следует производить резервное копирование и архивирование клиентских данных. Следуйте инструкциям в разделе [“Как задать роли для резервного копирования и архивирования данных клиента”](#) на стр. 115.

3. Укажите, когда следует производить резервное копирование и архивирование клиентских данных. Следуйте инструкциям в разделе [“Планирование операций резервного копирования и архивирования”](#) на стр. 119.
4. Чтобы позволить клиенту соединяться с сервером, зарегистрируйте клиент. Следуйте инструкциям в разделе [“Регистрация клиентов”](#) на стр. 120.
5. Чтобы начать защищать клиентский узел, установите и сконфигурируйте выбранную программу на клиентском узле. Следуйте инструкциям в разделе [“Установка и настройка клиентов”](#) на стр. 121.

Выбор программного обеспечения клиента и планирование установки

Для разных типов данных требуются разные типы защиты. Определите, какой тип данных вам нужно защищать, и выберите соответствующую программу.

Об этой задаче

Предпочтительная практика заключается в том, чтобы установить клиент резервного копирования и архивирования на всех клиентских узлах - тогда вы сможете сконфигурировать и запустить демон приемник клиента на клиентском узле. Приемник клиента разработан для эффективного выполнения запланированных операций.

Приемник клиента выполняет расписания для следующих продуктов: клиент резервного копирования и архивирования, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail и IBM Spectrum Protect for Virtual Environments. При установке продукта, для которого приемник клиента не выполняет расписания, вы должны следовать инструкциям по конфигурированию в документации по продукту, чтобы можно было выполнять запланированные операции.

Процедура

В зависимости от ваших целей выберите продукты, которые нужно установить, и ознакомьтесь с инструкциями по установке.

Совет: Если вы установите программу-клиент сейчас, вы, прежде чем сможете использовать клиент, также должны будете выполнить задачи по конфигурированию клиента, описанные в разделе [“Установка и настройка клиентов”](#) на стр. 121.

Цель	Продукт и описание	Инструкции по установке
Защитить файл-сервер или рабочую станцию	Клиент резервного копирования и архивирования производит резервное копирование и архивирование файлов и каталогов с файл-серверов и рабочих станций в систему хранения. Вы также можете восстанавливать и получать версии резервных копий и архивные копии файлов.	<ul style="list-style-type: none"> • Требования к среде клиента • Установить клиентов резервного копирования и архивирования UNIX и Linux • Первая установка клиента Windows
Защитить приложения с использованием резервного копирования снимков и возможностей восстановления	IBM Spectrum Protect Snapshot защищает данные с использованием интегрированного резервного копирования снимков и возможностей восстановления с учетом информации о приложениях. Вы можете защитить данные, которые хранятся в приложениях IBM программное обеспечение баз данных Db2 и SAP, Oracle, Microsoft Exchange и Microsoft SQL Server.	<ul style="list-style-type: none"> • Установка и обновление IBM Spectrum Protect Snapshot for UNIX and Linux • Установка и обновление IBM Spectrum Protect Snapshot for VMware • Установка и обновление IBM Spectrum Protect Snapshot for Windows

Цель	Продукт и описание	Инструкции по установке
Защитить приложение электронной почты на сервере IBM Domino	IBM Spectrum Protect for Mail: Data Protection for IBM Domino автоматизирует защиту данных, чтобы резервное копирование выполнялось без завершения работы серверов IBM Domino.	<ul style="list-style-type: none"> Установка Data Protection for IBM Domino в системе UNIX, AIX или Linux (V7.1.0) Установка Data Protection for IBM Domino в системе Windows (V7.1.0)
Защитить приложение электронной почты на сервере Microsoft Exchange	IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server автоматизирует защиту данных, чтобы резервное копирование выполнялось без завершения работы серверов Microsoft Exchange.	Установка, обновление и перенастройка IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
Защитить базу данных Db2	API (application programming interface, интерфейс прикладного программирования) клиента резервного копирования и архивирования можно использовать для резервного копирования данных Db2 на сервер IBM Spectrum Protect.	Установка клиентов резервного копирования и архивирования IBM Spectrum Protect (UNIX, Linux и Windows)
Защитить базу данных IBM Informix	API клиента резервного копирования и архивирования можно использовать для резервного копирования данных Informix на сервер IBM Spectrum Protect.	Установка клиентов резервного копирования и архивирования IBM Spectrum Protect (UNIX, Linux и Windows)
Защитить базу данных Microsoft SQL	IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server защищает данные Microsoft SQL.	Установка Data Protection for SQL Server в ядре сервера Windows
Защитить базу данных Oracle	IBM Spectrum Protect for Databases: Data Protection for Oracle защищает данные Oracle.	Установка Data Protection for Oracle
Защитить среду SAP	IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP обеспечивает защиту, настроенную для сред SAP. Продукт предназначен для того, чтобы повышать доступность серверов базы данных SAP и сокращать рабочую нагрузку администрирования.	<ul style="list-style-type: none"> Установка Data Protection for SAP for Db2 Установка Data Protection for SAP for Oracle

Цель	Продукт и описание	Инструкции по установке
Защитить виртуальную машину	<p>IBM Spectrum Protect for Virtual Environments обеспечивает защиту, настроенную для виртуальных сред Microsoft Hyper-V и VMware. IBM Spectrum Protect for Virtual Environments можно использовать для создания постоянных инкрементных резервных копий, хранящихся на централизованном сервере, создания политик резервного копирования и восстановления виртуальных машин или отдельных файлов.</p> <p>Либо используйте клиент резервного копирования и архивирования, чтобы производить резервное копирование и восстановление полной виртуальной машины VMware или Microsoft Hyper-V. Можно также производить резервное копирование и восстановление файлов или каталогов с виртуальной машины VMware.</p>	<ul style="list-style-type: none"> Установка и обновление Data Protection for Microsoft Hyper-V Установка и обновление Data Protection for VMware Установка клиентов резервного копирования и архивирования IBM Spectrum Protect (UNIX, Linux и Windows)

Совет: Чтобы использовать клиент для управления пространством, можно установить IBM Spectrum Protect for Space Management или IBM Spectrum Protect HSM for Windows.

Как задать роли для резервного копирования и архивирования данных клиента

Прежде чем вы добавите клиент, убедитесь, что соответствующие правила определены для поддержки и архивирования клиентских данных. В ходе процесса регистрации клиента вы назначается клиентский узел в домен политики, в котором есть правила, управляющие тем, как и когда производится сохранение данных клиента.

Прежде чем начать

Определитесь, как продолжать:

- Если вы знакомы с политиками, сконфигурированными для вашего решения, и вы знаете, что они не требуют изменений, то переходите к шагу [“Планирование операций резервного копирования и архивирования”](#) на стр. 119.
- Если вы не знакомы с политиками, то выполните шаги в этой процедуре.

Об этой задаче

Политики влияют на то, какой объем данных хранится в течение долгого времени и сколько времени данные сохраняются и будут доступны клиентам для восстановления. Для достижения целей для защиты данных можно обновить политику по умолчанию и создать собственные политики. Политика включает следующие правила:

- Как и когда производится резервное копирование и архивирование файлов в серверную систему хранения.
- Число копий файла и время хранения копий в серверной системе хранения.

В ходе процесса регистрации клиента вы назначается клиент в *домен политики*. Политика для отдельного клиента определяется правилами в домене политики, который назначен для клиента. В домене политики действующие правила находятся в активном *наборе политик*.

Когда клиент копирует или архивирует файл, файл привязывается к классу управления в активном наборе политик домена политики. *Класс управления* - это ключевой набор правил для управления данными клиента. Операции резервного копирования и архивирования на клиенте используют настройки в классе управления по умолчанию домена политики, если вы далее не настраиваете политику. Политику можно настроить, задав больше классов управления и назначив их использование через опции клиента.

Опции клиента можно задать в локальном, доступном для изменения файле в системе клиента и в наборе опций клиента на сервере. Опции в наборе опций клиента на сервере могут переопределять локальный файл опций клиента или могут добавлять в него опции.

Процедура

1. Ознакомьтесь с политиками, сконфигурированными для вашего решения - следуйте инструкциям в разделе [“Просмотр политик”](#) на стр. 116.
2. Чтобы внести незначительные изменения для соответствия требованиям хранения данных, следуйте инструкциям в разделе [“Изменение политик”](#) на стр. 116.
3. Необязательно: Если вам нужно создать домены политики или внести расширенные изменения в политики, чтобы выполнить требования к хранению данных, смотрите раздел [Настройка политик](#).

Просмотр политик

Просмотрите политики, чтобы определить, не нужно ли их изменить в соответствии с вашими требованиями.

Процедура

1. Чтобы просмотреть активный наборов политик для домена политики, сделайте следующее:
 - a) На странице **Службы** в Центре операций выберите домен политики и щелкните по **Сведения**.
 - b) На странице **Сводка** для домена политики щелкните по вкладке **Наборы политик**.

Совет: Чтобы облегчить возможность восстановления данных после атаки программы-вымогателя, следуйте инструкциям ниже:

- Убедитесь, что значение в столбце Резервные копии - это минимум 2. Предпочтительное значение - 3, 4 или более.
- Убедитесь, что значение в столбце Сохранять дополнительные резервные копии - это минимум 14 дней. Предпочтительное значение равно 30 или более дням.
- Убедитесь, что значение в столбце Сохранять архивы - это минимум 30 дней.

Если программа IBM Spectrum Protect for Space Management установлена на клиенте, то убедитесь, что создана резервная копия данных, перед тем как перемещать данные. В команде **DEFINE MGMTCLASS** или **UPDATE MGMTCLASS** задайте **MIGREQUIRESBKUP=YES**. Далее следуйте руководящим подсказкам.

2. Для просмотра бездействующих наборов политик для домена политики сделайте следующее:
 - a) На странице **Наборы политик** щелкните по **Конфигурировать**. Теперь можно просмотреть и изменить неактивные наборы политик.
 - b) Прокрутите неактивные наборы политик, используя стрелки Вперед и Назад. При просмотре неактивного набора политики параметры, которые отличают этот неактивный набор политик от активного набора политик, будут выделены.
 - c) Щелкните по переключателю **Конфигурировать**. Теперь наборы политик больше нельзя изменять.

Изменение политик

Чтобы изменить правила, применимые к домену политики, измените активный набор политик для домена политики. Можно также активировать для домена другой набор политик.

Прежде чем начать

Изменения политики могут повлиять на хранение данных. Убедитесь, чтобы вы продолжаете резервное копирование данных, имеющих существенное значение для вашей организации, чтобы можно было восстановить эти данные, если произойдет бедствие. Также убедитесь, что в вашей системе достаточно пространства хранения для запланированных операций резервного копирования.

Об этой задаче

Вы изменяете набор политик, изменяя один или несколько классов управления в наборе политик. Если вы измените активный набор политик, изменения не будут доступны клиентам, пока вы не активируете повторно набор политик. Чтобы сделать измененный набор политик доступным клиентам, активируйте набор политик.

Хотя для домена политики можно задать несколько наборов политик, активным может быть только один набор политик. При активации другого набора политики он заменяет активный в данный момент набор политик.

Предпочтительный опыт определения политик описан в разделе [Настройка политик](#).

Процедура

1. На странице **Службы** в Центре операций выберите домен политики и щелкните по **Сведения**.
2. На странице **Сводка** для домена политики щелкните по вкладке **Наборы политик**.

На странице **Наборы политик** указано имя активного набора политики и перечислены все классы управления для этого набора политик.

3. Щелкните по переключателю **Конфигурировать**. Набор политик доступен для изменения.
4. Чтобы изменить неактивный набор политик, щелкните по стрелкам вперед и назад, чтобы найти набор политик.
5. Измените набор политик, выполнив любое из следующих действий:

Опция	Описание
Добавьте класс управления	<p>a. В таблице Наборы политик щелкните по +Класс управления.</p> <p>b. Чтобы задать правила для резервного копирования и архивирования данных, заполните поля в окне Добавить класс управления.</p> <p>c. Чтобы сделать класс управления классом управления по умолчанию, включите переключатель Сделать значением по умолчанию.</p> <p>d. Щелкните по Добавить.</p>
Удалите класс управления	<p>В столбце Класс управления щелкните по -.</p> <p>Совет: Чтобы удалить класс управления по умолчанию, нужно сначала назначить другой класс управления классом управления по умолчанию.</p>
Сделать класс управления классом управления по умолчанию	<p>Щелкните по радиокнопке в столбце Значение по умолчанию для класса управления.</p> <p>Совет: Класс управления по умолчанию управляет файлами клиента, если для файла не назначен другой класс управления или если класс управления файла не подходит для управления файлом. Чтобы убедиться в том, что клиенты всегда могут производить резервное копирование и архивирование файлов, выберите класс управления по умолчанию и для резервного копирования, и для архивирования файлов.</p>

Опция	Описание
Изменить класс управления	Чтобы изменить свойства класса управления, обновите поля в таблице.

6. Щелкните по **Сохранить**.



Внимание: При активации нового набора политик можно потерять данные. Данные, защищенные в соответствии с одним набором политик, могут оказаться незащищенными с точки зрения другого набора политик. Поэтому, прежде чем активировать набор политик, убедитесь, что разница между предыдущим набором политик и новым набором политик не вызовет потерю данных.

7. Выберите **Активировать**. Будет показана сводка различий между активным набором политик и новым набором политик. Убедитесь, что изменения в новом наборе политики совместимы с вашими требованиями к хранению данных; для этого выполните следующие шаги:

- Проверьте различия между соответствующими классами управления в двух наборах политик и рассмотрите последствия для файлов клиентов. Файлы клиентов, связанные с классами управления в активном наборе политик, будут связаны с классами управления с теми же именами в новом наборе политик.
- Укажите в активном наборе политики классы управления, у которых нет эквивалентов в новом наборе политики, и рассмотрите последствия для файлов клиента. Файлы клиентов, связанные с этими классами управления, будут управляться классом управления по умолчанию в новом наборе политик.
- Если изменения, которые должны быть реализованы набором политики, являются допустимыми, выберите переключатель **Я понимаю, что эти обновления могут вызвать потерю данных** и щелкните по **Активировать**.

Изменение объема резервного копирования клиента

При настройке операций резервного копирования клиента предпочтительной практикой является исключение объектов, которые вам не требуются. Например, обычно имеет смысл исключить из операции резервного копирования временные файлы.

Об этой задаче

Исключение ненужных объектов из операций резервного копирования позволяет лучше контролировать объем пространства хранения, необходимого для операций резервного копирования, а также расходы на хранение. В зависимости от вашего пакета лицензирования вам, возможно, также удастся ограничить расходы, связанные с лицензированием.

Процедура

То, как вы изменяете масштаб операций по резервному копированию, зависит от продукта, установленного на клиентском узле:

- Для клиента резервного копирования и архивирования можно создать список включения-исключения, чтобы включить файлы, группы файлов или каталоги в операции резервного копирования или исключить их из этих операций. Чтобы создать список включения-исключения, следуйте инструкциям в разделе [Создание списка include-exclude](#).

Чтобы обеспечить непротиворечивое использование списка включения-исключения для всех клиентов одного типа, можно создать на сервере набор опций клиента, содержащий необходимые опции. Затем вы назначаете набор опций клиента каждому из клиентов того же типа. Дополнительные сведения смотрите в разделе [Управление операциями клиента через наборы опций клиентов](#).

- Для клиента резервного копирования и архивирования можно задать объекты в операции инкрементного резервного копирования, используя опцию **domain**. Следуйте инструкциям в разделе [Domain, опция](#).

- В случае других продуктов, чтобы указать, какие объекты включаются в операции резервного копирования, а какие - исключаются из этих операций, следуйте инструкциям в документации по продукту.

Планирование операций резервного копирования и архивирования

Прежде чем зарегистрировать новый клиент на сервере, убедитесь, что существует расписание, позволяющее указать, когда выполняются операции резервного копирования и архивирования. В процессе регистрации можно назначить расписание клиенту.

Прежде чем начать

Определитесь, как продолжать:

- Если вы знакомы с расписаниями, сконфигурированными для вашего решения, и вы знаете, что они не требуют изменений, то переходите к шагу [“Регистрация клиентов”](#) на стр. 120.
- Если вы не знакомы с расписаниями или расписания нужно изменить, выполните шаги в этой процедуре.


Об этой задаче

Как правило, операции резервного копирования для всех клиентов должны выполняться ежедневно. Спланируйте рабочую нагрузку клиента и сервера, чтобы обеспечить наивысшую производительность для вашей среды хранения. Чтобы избежать перекрывания операций клиента и сервера, рассмотрите возможность запланировать выполнение операций резервного копирования и архивирования клиента по ночам. Если операции клиента и сервера будут перекрываться или для их обработки не выделят достаточно времени и ресурсов, то вы можете столкнуться со снижением производительности системы, неудачным завершением операций и другими проблемами.

Процедура

1. Проверьте доступные расписания, установив указатель мыши на **Клиенты** в строке меню Центра операций. Щелкните по **Расписания**.
2. Необязательно: Измените или создайте расписание, выполнив следующие шаги:

Опция	Описание
Изменение расписания	<p>a. В представлении Расписания выберите расписание и щелкните по Сведения.</p> <p>b. На странице Сведения о расписании просмотрите сведения, щелкнув по синим стрелкам в начале строк.</p> <p>c. Измените параметры в расписании и нажмите на Сохранить.</p>
Создание расписания	В представлении Расписания щелкните по +Расписание и выполните шаги по созданию расписания.

3. Необязательно: Чтобы сконфигурировать параметры расписания, которые не видны в компоненте Центр операций, используйте серверную команду. Например, вы можете счесть целесообразным запланировать операцию клиента, которая создает резервную копию определенного каталога и назначает для него класс управления, отличающийся от класса управления по умолчанию.
 - a) На странице **Обзор** в компоненте Центр операций установите указатель мыши на значок параметров  и щелкните по **Построитель команд**.
 - b) Введите команду **DEFINE SCHEDULE**, чтобы создать расписание, или команду **UPDATE SCHEDULE**, чтобы изменить расписание. Дополнительные сведения о командах смотрите в разделах [DEFINE SCHEDULE \(Задать запланированное задание клиента\)](#) или [UPDATE SCHEDULE \(Изменить запланированное задание клиента\)](#).

Информация, связанная с данной

[Настройка расписания для ежедневных операций](#)

Регистрация клиентов

Зарегистрируйте клиент, чтобы убедиться, что он может соединиться с сервером, а сервер может защитить данные клиента.

Прежде чем начать

Узнайте, нужен ли клиенту ID администратора с правами владельца клиента в клиентском узле. Чтобы узнать, каким клиентам требуется ID администратора, смотрите публикацию [technote 7048963](#).

Ограничение: Для клиентов некоторых типов требуется совпадение имени клиентского узла и ID администратора. Этих клиентов невозможно аутентифицировать с помощью метода Lightweight Directory Access Protocol (LDAP), внедренного в версии 7.1.7. Подробную информацию об этом методе аутентификации, который иногда называется интегрированным режимом, смотрите в документе [Аутентификация пользователей с использованием базы данных Active Directory](#).

Процедура

Чтобы зарегистрировать клиент, выполните одно из следующих действий:

- Если клиенту требуется ID администратора, то зарегистрируйте клиент с помощью команды **REGISTER NODE** и задайте параметр **USERID**:

```
register node имя_узла пароль userid=имя_узла
```

где *имя_узла* - это имя узла и *пароль* - это пароль узла. Дополнительные сведения смотрите в разделе [Регистрация узла](#).

- Если клиенту требуется ID администратора, то зарегистрируйте клиент с помощью мастера добавления клиента Центра операций. Сделайте следующее:
 - В строке меню компонента Центр операций выберите **Клиенты**.
 - В таблице Клиенты щелкните по **+ Клиент**.
 - Выполните шаги в мастере **Добавить клиент**:
 - Укажите, что избыточные данные можно устранить как на клиенте, так и на сервере. Выберите переключатель **Включить** в области Дедупликация данных на стороне клиента.
 - В окне **Конфигурация** скопируйте значения **TCPSERVERADDRESS**, **TCPPORT**, **NODENAME**, и **DEDUPLICATION**.

Совет: Запишите значения опций и сохраните их в надежном месте. По завершении регистрации клиента и установки программы на клиентском узле используйте значения для конфигурирования клиента.
 - Следуйте инструкциям в мастере, чтобы задать домен политики, расписание и набор опций.
 - Укажите, как для клиента будут показаны риски, задав параметр Под угрозой.
 - Щелкните по **Добавить клиент**.

Информация, связанная с данной

[Опция Tcpserveraddress](#)

[Опция Tcpsport](#)

[Опция Nodename](#)

[Опция дедупликации](#)

Установка и настройка клиентов

Чтобы начать защищать клиентский узел, нужно установить и сконфигурировать выбранную программу.

Процедура

Если вы уже установили программу, то начните с шага “2” на стр. 122.

1. Выполните одно из следующих действий.

- Чтобы установить программу в приложении или на клиентском узле, выполните инструкции.

Программа	Ссылка на инструкции
Клиент резервного копирования и архивирования IBM Spectrum Protect	<ul style="list-style-type: none">– Установить клиентов резервного копирования и архивирования UNIX и Linux– Первая установка клиента Windows <p>Совет: Можно также обновить существующие клиенты при помощи Центра операций. Инструкции смотрите в разделе Планирование обновлений клиентов.</p>
IBM Spectrum Protect for Databases	<ul style="list-style-type: none">– Установка Data Protection for Oracle– Установка Data Protection for SQL Server в ядре сервера Windows
IBM Spectrum Protect for Mail	<ul style="list-style-type: none">– Установка Data Protection for IBM Domino в системе UNIX, AIX или Linux (V7.1.0)– Установка Data Protection for IBM Domino в системе Windows (V7.1.0)– Установка, обновление и перенастройка IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect Snapshot	<ul style="list-style-type: none">– Установка и обновление IBM Spectrum Protect Snapshot for UNIX and Linux– Установка и обновление IBM Spectrum Protect Snapshot for VMware– Установка и обновление IBM Spectrum Protect Snapshot for Windows
IBM Spectrum Protect for Enterprise Resource Planning	<ul style="list-style-type: none">– Установка Data Protection for SAP for Db2– Установка Data Protection for SAP for Oracle

- Чтобы установить программу на клиентском узле виртуальной машины, выполните инструкции для выбранного типа резервного копирования.

Тип резервного копирования	Ссылка на инструкции
Если вы собираетесь создавать полные резервные копии VMware виртуальных машин, установите и сконфигурируйте клиент резервного копирования и архивирования IBM Spectrum Protect.	<ul style="list-style-type: none">– Установить клиентов резервного копирования и архивирования UNIX и Linux– Первая установка клиента Windows

Тип резервного копирования	Ссылка на инструкции
Если вы собираетесь установить постоянные полные резервные копии виртуальных машин, установите и сконфигурируйте IBM Spectrum Protect for Virtual Environments и клиент резервного копирования и архивирования на одном и том же клиентском узле или на разных клиентских узлах.	<p>– Защита данных для VMware</p> <p>Совет: Программу для IBM Spectrum Protect for Virtual Environments и для клиента резервного копирования и архивирования можно получить в пакете установки IBM Spectrum Protect for Virtual Environments.</p>

2. Чтобы разрешить клиенту соединиться с сервером, добавьте или обновите значения опций **TCPSEVERADDRESS**, **TCPPORT** и **NODENAME** в файле опций клиента. Используйте значения, записанные при регистрации клиента (раздел [“Регистрация клиентов”](#) на стр. 120).

- Если клиенты установлены в операционной системе AIX, Linux или Mac OS X, добавьте значения в файл системных опций клиента, `dsm.sys`.
- Если клиенты установлены в операционной системе Windows, добавьте значения в файл `dsm.opt`.

По умолчанию, файлы опций находятся в каталоге установки.

3. Необязательно: Если вы установили клиент резервного копирования и архивирования в операционной системе Linux или Windows, то установите службу управления клиентами на клиенте. Следуйте инструкциям в разделе [Установка службы управления клиентом](#).
4. Сконфигурируйте клиент для выполнения запланированных операций. Следуйте инструкциям в разделе [“Конфигурирование клиента для выполнения запланированных операций”](#) на стр. 122.
5. Необязательно: Сконфигурируйте связь через брандмауэр. Следуйте инструкциям в разделе [“Конфигурирование взаимодействий между клиентом и сервером через брандмауэр”](#) на стр. 125.
6. Запустите тестовое резервное копирование, чтобы проверить, защищены ли данные, как вы планировали.
Например, для клиента резервного копирования и архивирования выполните следующие шаги:
 - а) Выберите на странице **Клиенты** компонента Центр операций клиент, для которого вы хотите выполнить резервное копирование, и щелкните по **Резервное копирование**.
 - б) Убедитесь, что резервное копирование выполнено успешно и что нет ни предупреждений, ни сообщений об ошибках.
7. Следите за результатами запланированных операций клиента в компоненте Центр операций.

Дальнейшие действия

Чтобы изменить набор объектов для резервного копирования из клиента, выполните инструкции в разделе [“Изменение объема резервного копирования клиента”](#) на стр. 118.

Конфигурирование клиента для выполнения запланированных операций

Вы должны сконфигурировать и запустить планировщик клиента на клиентском узле. Планировщик клиента обеспечивает взаимодействие между клиентом и сервером, чтобы могли выполняться запланированные операции. Например, запланированные операции обычно включают в себя резервное копирование файлов с клиента.

Об этой задаче

Предпочтительный метод заключается в том, чтобы установить клиент резервного копирования и архивирования на всех клиентских узлах - тогда вы сможете сконфигурировать и запустить

приемник клиента на клиентском узле. Приемник клиента разработан для эффективного выполнения запланированных операций. Приемник клиента управляет планировщиком клиента, чтобы планировщик запускался, только когда это требуется:

- Когда наступило время запросить сервер о следующей запланированной операции
- Когда наступило время запустить следующую запланированную операцию

Используя приемник клиента, вы можете сократить число фоновых процессов на клиенте и помочь избежать проблем сохранения памяти.

Приемник клиента выполняет расписания для следующих продуктов: клиент резервного копирования и архивирования, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail и IBM Spectrum Protect for Virtual Environments. При установке продукта, для которого приемник клиента не выполняет расписания, следуйте инструкциям по конфигурированию в документации по продукту, чтобы можно было выполнять запланированные операции.

Если на вашем предприятии используется сторонний инструмент планирования в качестве стандартной практики, можно использовать этот инструмент планирования как альтернативу приемнику клиентов. Как правило, сторонние инструменты планирования запускают программы-клиенты напрямую, используя команды операционной системы. Чтобы сконфигурировать сторонний инструмент планирования, смотрите документацию по продукту.

Процедура

Чтобы сконфигурировать и запустить планировщик клиента с использованием приемника клиента, следуйте инструкциям для операционной системы, установленной на клиентском узле:

AIX и Oracle Solaris

- а. В графическом пользовательском интерфейсе клиента резервного копирования и архивирования выберите **Изменить > Предпочтения клиента**.
- б. Щелкните по вкладке **Веб-клиент**.
- в. В поле **Опции управляемых служб** щелкните по **Расписание**. Если вы также хотите, чтобы приемник клиента управлял веб-клиентом, щелкните по опции **И то, и другое**.
- г. Чтобы убедиться, что планировщик может запуститься без участия оператора, задайте для опции **passwordaccess** в файле `dsm.sys` значение `generate`.
- д. Чтобы сохранить пароль клиентского узла, введите следующую команду и укажите пароль клиентского узла, когда вам это предложат:

```
dsmc query sess
```

- ф. Запустите приемник клиента, введя в командной строке следующую команду:

```
/usr/bin/dsmcad
```

- г. Чтобы включить автоматический запуск приемника клиента после перезапуска системы, добавьте в файл запуска системы (обычно, `/etc/inittab`) следующую запись:

```
tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # Демон Client Acceptor
```

Linux

- а. В графическом пользовательском интерфейсе клиента резервного копирования и архивирования выберите **Изменить > Предпочтения клиента**.
- б. Щелкните по вкладке **Веб-клиент**.
- в. В поле **Опции управляемых служб** щелкните по **Расписание**. Если вы также хотите, чтобы приемник клиента управлял веб-клиентом, щелкните по опции **И то, и другое**.
- г. Чтобы убедиться, что планировщик может запуститься без участия оператора, задайте для опции **passwordaccess** в файле `dsm.sys` значение `generate`.

- e. Чтобы сохранить пароль клиентского узла, введите следующую команду и укажите пароль клиентского узла, когда вам это предложат:

```
dsmc query sess
```

- f. Запустите приемник клиента, войдя в систему от имени ID пользователя root и введя следующую команду:

```
service dsmcad start
```

- g. Чтобы включить автоматический запуск приемника клиента после перезапуска системы, добавьте службу, введя в командной строке оболочки следующую команду:

```
# chkconfig --add dsmcad
```

MAC OS X

- В графическом пользовательском интерфейсе клиента резервного копирования и архивирования выберите **Изменить > Предпочтения клиента**.
- Чтобы планировщик мог запускаться без участия оператора, щелкните по **Авторизация**, выберите **Генерирование пароля** и щелкните по **Применить**.
- Чтобы указать, как осуществляется управление службами, щелкните по **Веб-клиент**, выберите **Расписание**, щелкните по **Применить** и выберите **ОК**.
- Чтобы сгенерированный пароль был сохранен, перезапустите клиент резервного копирования и архивирования.
- Используйте для запуска приемника клиента приложение Инструменты IBM Spectrum Protect для администраторов.

Windows

- В графическом пользовательском интерфейсе клиента резервного копирования и архивирования выберите **Утилиты > Мастер настройки > Помочь мне сконфигурировать Планировщик клиента**. Щелкните по **Далее**.
- Прочтите информации на странице **мастера планировщика** и нажмите **Далее**.
- На странице **Задача планировщика** выберите **Установить новый или дополнительный планировщик** и нажмите **Далее**.
- На странице **Имя и расположение планировщика** задайте имя для добавляемого планировщика клиента. Затем выберите **Использовать Client Acceptor Daemon (CAD)**, чтобы управлять планировщиком, и нажмите **Далее**.
- Введите имя, которое вы хотите присвоить этому приемнику клиента. Имя по умолчанию - Client Acceptor. Щелкните по **Далее**.
- Выполните конфигурирование, выполняя шаги в мастере.
- Обновите файл опций клиента, `dsm.opt`, и задайте для опции **passwordaccess** значение `generate`.
- Чтобы сохранить пароль клиентского узла, введите в командной строке следующую команду:

```
dsmc query sess
```

Когда вам это предложат, введите пароль клиентского узла.

- Запустите службу приемника клиента из панели **Управление службами**. Например, если вы использовали имя по умолчанию, запустите Служба Client Acceptor. Не запускайте службу планировщика, заданную вами на странице **Имя и местонахождение планировщика**. Служба планировщика автоматически запускается и останавливается службой приемника клиента по мере необходимости.

Конфигурирование взаимодействий между клиентом и сервером через брандмауэр

Если клиент должен связываться с сервером через брандмауэр, нужно включить связь между клиентом и сервером через брандмауэр.

Прежде чем начать

Если для регистрации клиентов вы использовали мастер добавления клиентов, найдите в файле опций клиента значения опций, полученные вами в ходе этого процесса. Для указания портов можно использовать значения.

Об этой задаче



Внимание: Не конфигурируйте брандмауэр, используя метод, который мог бы вызвать прекращение сеансов, используемых сервером или агентом хранения. Прекращение действительного сеанса может вызвать непредсказуемые последствия. Может показаться, что процессы и сеансы остановились из-за ошибок ввода-вывода. Чтобы помочь исключить сеансы из ограничений тайм-аута, сконфигурируйте известные порты для компонентов IBM Spectrum Protect. Убедитесь, что для серверной опции **KEEPALIVE** осталось заданным значение по умолчанию YES. Это поможет вам убедиться, что связи клиент/сервер не прерывается. Инструкции относительно того, как задать опцию сервера **KEEPALIVE** смотрите в разделе [KEEPALIVE](#).

Процедура

Откройте следующие порты, чтобы разрешить доступ через брандмауэр:

Порт TCP/IP для клиента резервного копирования и архивирования, административного клиента командной строки и планировщика клиента

Задайте порт, используя опцию **tcpport** в файле опций клиента. Опция **tcpport** в файле опций клиента должна совпадать с опцией **TCPPORT** в файле опций сервера. Значение по умолчанию - 1500. Если вы решите использовать какое-либо значение, отличающееся от значения по умолчанию, задайте число в диапазоне 1024-32767.

Порт HTTP для включения взаимодействий между веб-клиентом и удаленными рабочими станциями

Задайте порт для удаленной рабочей станции, задав опцию **httpport** в файле опций клиента удаленной рабочей станции. Значение по умолчанию - 1581.

Порты TCP/IP для удаленной рабочей станции

Значение по умолчанию равно 0 (ноль); оно указывает, что два свободных номера портов случайным образом назначаются удаленной рабочей станции. Если вы не хотите, чтобы номера портов назначались произвольным образом, задайте значения, задав опцию **webports** в файле опций клиента удаленной рабочей станции.

Порт TCP/IP для сеансов администрирования

Задайте порт, на котором сервер ожидает требований установления сеансов административного клиента. Значение опции клиента **tcpadminport** должно совпадать с опцией сервера **TCPADMINPORT**. Таким способом вы сможете защитить административные сеансы в частной сети.

Конфигурирование перемещения данных в режиме без сети;

Можно сконфигурировать клиент и сервер так, чтобы клиент мог переместить данные через агент хранения непосредственно в систему хранения в сети хранения данных (SAN).


Об этой задаче

Перемещение данных в режиме без локальной сети предоставляется продуктом IBM Spectrum Protect for SAN. Дополнительную информацию смотрите в документации к [IBM Spectrum Protect for SAN](#).

Процедура

Чтобы сконфигурировать перемещение данных без локальной сети, выполните следующие шаги.

1. Проверьте сетевое соединение.
2. Установите связь между клиентом, агентом хранения и сервером.
3. Установите и сконфигурируйте программное обеспечение систем клиентов.
4. Сконфигурируйте на сервере устройства, к которым будет обращаться агент хранения.
5. Сконфигурируйте политики перемещения данных в режиме без локальной сети IBM Spectrum Protect для клиента.
6. При работе с совместно используемой системой хранения FILE установите и сконфигурируйте IBM TotalStorage SAN File System или IBM Spectrum Scale.

Ограничение:  Если том IBM Spectrum Scale сформатирован сервером AIX, система Windows использует для передачи данных TCP/IP, а не сеть хранения данных (storage area network, SAN).

7. Определите пути от агента хранения к накопителям.
8. Запустите агент хранения и проверьте конфигурацию без локальной сети.

Дальнейшие действия

Для упрощения настройки ресурсов локальной сети и сети хранения можно контролировать пути перемещения данных для клиентов с функцией перемещения данных в режиме без локальной сети. Чтобы управлять путем, используйте команду **UPDATE NODE**. Для каждого клиента можно выбрать для операций чтения и записи данных один из следующих параметров. Задайте операции чтения данных, используя параметр **DATAREADPATH**, и операции записи данных, используя параметр **DATAWRITEPATH**. Это необязательный параметр. Значение по умолчанию - ANY.

LAN (только путь в локальной сети)

Задайте значение LAN, если выполняется любое из следующих условий:

- Вы хотите произвести резервное копирования или восстановление небольшого объема данных.
- У клиента нет соединений SAN.

LANFREE (только путь без локальной сети)

Задайте значение LANFREE, если клиент и сервер находится в одной и той же SAN и если выполняется любое из следующих условий:

- Вы хотите произвести резервное копирования или восстановление большого объема данных.
- Вы хотите выгрузить нагрузку по серверной обработке на клиент.
- Вы хотите снять конфликты локальной сети.

ANY (любой доступный путь)

Если доступен путь без локальной сети, то он будет использован. Если путь без локальной сети недоступен, данные будут перемещены через локальную сеть.

Проверка конфигурации для использования режима без локальной сети

После конфигурирования клиента IBM Spectrum Protect для перемещения данных в режиме без локальной сети можно проверить конфигурацию и определения сервера при помощи команды **VALIDATE LANFREE**.

Об этой задаче

Команда **VALIDATE LANFREE** позволяет определить, какие объекты назначения для узла, использующего конкретный агент хранения, допускают перемещение данных в режиме без локальной сети. Вывод этой команды помогает определить также, есть ли проблемы с существующей конфигурацией в режиме без локальной сети. Можно оценить политику, пул хранения и определения путей для узла и используемого им агента хранения, чтобы убедиться, что операция выполняется должным образом.

Процедура

- Определите, нет ли у клиентского узла проблемы с его конфигурацией без локальной сети; для этого введите команду **VALIDATE LANFREE**. Например, если клиентский узел FRED использует агент хранения FRED_STA, введите следующую команду:

```
validate lanfree fred fred_sta
```

Результаты помогут вам выявить корректировки, которые могут потребоваться в конфигурации или политике хранения. Выходная информация показывает, какие назначения классов управления для того или иного типа операций не поддерживают передачу данных в режиме без локальной сети. Сообщается также об общем количестве объектов назначения в режиме без локальной сети.

Информация, связанная с данной

[VALIDATE LANFREE \(проверка путей в режиме без локальной сети\)](#)

Методы шифрования лент

Выбор используемого метода шифрования зависит от планируемого способа управления данными.

Крайне важно защитить данные клиента, особенно, если эти данные - конфиденциальные. Чтобы гарантировать защиту данных на томах на площадке и вне площадки, существует технология шифрования лент IBM.

Эта технология использует более высокий уровень шифрования, для которого требуются 256-разрядные ключи шифрования стандарта AES (Advanced Encryption Standard). Ключи передаются на накопитель менеджером ключей, чтобы производить шифрование и расшифровку данных.

Ленточная технология IBM поддерживает разные методы шифрования накопителей для следующих устройств:

- IBM 3592 поколений 2 и 3
- IBM Linear Tape Open поколений 4 и 5

Методы шифрования накопителей, которые можно использовать в сочетании с IBM Spectrum Protect, конфигурируются на аппаратном уровне. IBM Spectrum Protect не может ни задать, ни изменить метод шифрования, используемый в аппаратной конфигурации. Если оборудование настроено для метода приложений, IBM Spectrum Protect может включить или выключить шифрование в зависимости от значения **DRIVEENCRYPTION** для класса устройств.

Чтобы зашифровать все данные в отдельной логической библиотеке или зашифровать данные более чем на одном томе пула хранения, используйте метод Библиотека или Система. Если менеджер ключей шифрования настроен для совместного использования ключей, методы Библиотека и Система могут совместно использовать ключ шифрования, обеспечивая взаимозаменяемость этих двух методов. IBM Spectrum Protect не может совместно использовать или отдельно использовать ключи шифрования из метода Приложение и либо метода шифрования Библиотека, либо либо метода шифрования Система.

Таблица 24. Методы шифрования

Метод шифрования	Описание
Шифрование на уровне приложения	<p>Используя шифрование, управляемое приложением, можно создать отдельные пулы хранения, содержащие только зашифрованные тома. Таким образом можно использовать иерархии и политики пулов хранения для управления способом шифрования данных.</p> <p>Ключами шифрования управляет приложение, в данном случае, IBM Spectrum Protect. IBM Spectrum Protect генерирует и хранит ключи в базе данных сервера. Шифруются данные во время операций записи, когда ключ шифрования передается с сервера на накопитель. Для операций чтения данные расшифровываются.</p> <p>Чтобы зашифровать тома пула хранения и устранить часть обработки шифрования в системе, включите метод Приложение. Используйте шифрование, управляемое приложением, только для томов пула хранения. Другие тома, например, ленты с наборами резервных копий, жкспортируемые тома и резервные копии базы данных, не шифруются с использованием метода Приложение.</p> <p>Требование: Если включено шифрование приложений, вы должны особо тщательно подходить к защите резервных копий базы данных, так как ключи шифрования, используемые для шифрования и расшифровки данных, хранятся в базе данных сервера. Для восстановления данных необходимо иметь правильную резервную копию базы данных и соответствующие ключи шифрования для доступа к информации. Во избежание потери или кражи данных следует часто создавать резервные копии базы данных и обеспечивать их безопасность. Любой пользователь, имеющий доступ к резервной копии базы данных и ключам шифрования, получит доступ к вашим данным.</p>

Таблица 24. Методы шифрования (продолжение)	
Метод шифрования	Описание
Шифрование на уровне библиотеки	<p>Используя управляемое библиотекой шифрование, можно управлять тем, какие тома будут зашифрованы с использованием их серийных номеров. Можно задать диапазон или набор томов, которые необходимо шифровать.</p> <p>Ключами шифрования управляет библиотека. Они хранятся в менеджере ключей шифрования и передаются на накопитель. Если вы настроите оборудование для использования шифрования, управляемого библиотекой, вы сможете использовать этот метод, выполнив команду DEFINE DEVCLASS и задав параметр DRIVEENCRYPTION=ALLOW.</p> <p>Ограничение: Только некоторые библиотеки IBM поддерживают шифрование IBM LTO-4 и новее. Дополнительную информацию смотрите в разделе “Конфигурирование шифрования ленточных накопителей” на стр. 129.</p>
Шифрование на уровне системы	<p>Управляемое системой шифрование доступно только в операционной системе AIX®. Ключами шифрования, которые передаются накопителю, управляет драйвер устройства или операционная система, а хранятся они в менеджере ключей шифрования. Если оборудование настроено для использования системного шифрования, вы сможете использовать этот метод, выполнив команду DEFINE DEVCLASS и задав параметр DRIVEENCRYPTION=ALLOW.</p>

Чтобы определить, зашифрован ли том и какой метод использовался, выполните команду **QUERY VOLUME** и задайте параметр **FORMAT=DETAILED**.

Конфигурирование шифрования ленточных накопителей

Шифрование накопителей можно использовать для защиты лент, содержащих важные или конфиденциальные данные (например, лент с конфиденциальной финансовой информацией). Шифрование накопителей может быть полезно, если вы перемещаете ленты из среды сервера IBM Spectrum Protect в расположение на площадке или вне площадки.

Об этой задаче

Чтобы определить, какие методы шифрования можно использовать при работе с различными типами накопителей, смотрите следующую таблицу.

Таблица 25. Доступные методы шифрования			
	На уровне программы	На уровне библиотеки	На уровне системы
3592 поколения 2 и новее	Да	Да.	Да
HP LTO-4 и новее	Да	Нет.	Нет

Таблица 25. Доступные методы шифрования (продолжение)

	На уровне программы	На уровне библиотеки	На уровне системы
IBM LTO-4 и новее	Да	Да, но только если ваше оборудование системы (например, ленточная библиотека TS3500), это поддерживает.	Да
Oracle StorageTek T10000B	Да	Нет.	Нет
Oracle StorageTek T10000C	Да	Нет.	Нет
Oracle StorageTek T10000D	Да	Нет.	Нет

В библиотеке могут содержаться накопители разных типов, часть которых будет поддерживать шифрование, а часть - нет. Например, в библиотеке могут содержаться два накопителя LTO-2, два накопителя LTO-3 и два накопителя LTO-4. Комбинация разных типов носителей в библиотеке также может образоваться вследствие использования различных шифруемых и нешифруемых классов устройств с разными технологиями лент и накопителей.

ограничения:

- Чтобы применить шифрование к накопителям LTO-4 или новее, все накопители должны поддерживать шифрование.
- Чтобы применить шифрование к логической библиотеке, следует использовать один и тот же метод шифрования для всех накопителей в библиотеке. Не создавайте среду, в которой для некоторых накопителей используется метод шифрования на уровне программы, а для других — на уровне библиотеки или системы.

Более подробную информацию о настройке аппаратной среды для использования шифрования накопителей смотрите в документации по соответствующему оборудованию.

Процедура

1. Установите драйвер устройств, поддерживающий шифрование накопителей:
 - Чтобы активировать шифрование для накопителя IBM LTO-4 или новее, нужно установить драйвер устройств IBM RMSS Ultrium. Накопители SCSI не поддерживают шифрование IBM LTO-4 или новее.
 - Чтобы активировать шифрование для HP LTO-4 или новее, нужно установить драйвер устройств IBM Spectrum Protect.
2. Включите шифрование для накопителя, задав параметр **DRIVEENCRYPTION** в команде **DEFINE DEVCLASS** или **UPDATE DEVCLASS** для типов устройств 3592, LTO или ECARTRIDGE.

Дальнейшие действия

При использовании накопителей, для которых доступен поддерживаемый метод шифрования, для записи данных на ленты используется другой формат. Если данные записываются на тома с использованием другого формата и если тома затем возвращаются в чистое состояние, они будут содержать метки, которые смогут прочитать только накопители, поддерживающие шифрование. Чтобы использовать такие чистые тома в накопителях, не поддерживающих шифрование (когда оборудование не поддерживает шифрование или установлен метод шифрования NONE), тома необходимо перемаркировать.

Задачи, связанные с данной

Как включить и выключить шифрование накопителей 3592 поколения 2 и новее

При работе с IBM Spectrum Protect можно использовать следующие типы шифрования накопителей для накопителей 3592 второго и последующих поколений: шифрование на уровне программ, системы и библиотеки. Эти методы конфигурируются на аппаратном уровне.

Как включить и выключить шифрование накопителей для ленточных накопителей LTO поколения 4 или новее

IBM Spectrum Protect поддерживает три типа шифрования накопителей, которые доступны для накопителей LTO поколения 4 или новее: шифрование на уровне приложений, системы и библиотеки (Приложение, Система и Библиотека). Эти методы конфигурируются на аппаратном уровне.

Информация, связанная с данной

DEFINE DEVCLASS (Задать класс устройств)

UPDATE DEVCLASS (изменение класса устройства)

Управление операциями ленточного хранения

В определениях классов устройств для ленточных устройств есть параметры, позволяющие управлять операциями хранения.

Как IBM Spectrum Protect заполняет тома

Команда **DEFINE DEVCLASS** имеет необязательный параметр **ESTCAPACITY**, который показывает примерную емкость томов с последовательным доступом, связанных с классом устройства. В IBM Spectrum Protect примерная емкость томов используется для оценки емкости пула хранения данных и процента используемого пространства.

Если параметр **ESTCAPACITY** не задан, IBM Spectrum Protect использует значение по умолчанию, основываясь на формате записи, который указан для класса устройства (параметр **FORMAT=**).

Если указать примерную емкость, которая превышает фактическую емкость тома в классе устройства, IBM Spectrum Protect обновит примерную емкость тома при его заполнении. Когда IBM Spectrum Protect заполнит том полностью, произойдет обновление емкости в соответствии с объемом, записанным в том.

Можно принять стандартное значение примерной емкости для класса устройства или явно указать примерную емкость. Точное значение примерной емкости не требуется, но рекомендуется. В IBM Spectrum Protect примерная емкость томов используется для оценки емкости пула хранения данных и процента используемого пространства. Примерную емкость может понадобиться изменить в следующих случаях:

- Примерная емкость по умолчанию неточна из-за сжатия данных.
- Используются тома нестандартного размера.

Информация, связанная с данной

DEFINE DEVCLASS (Задать класс устройств)

UPDATE DEVCLASS (изменение класса устройства)

Указание оценочной емкости ленточных томов

В IBM Spectrum Protect примерная емкость используется также для определения времени начала освобождения томов пула хранения.

Об этой задаче

Для классов ленточных устройств выбранные сервером значения по умолчанию зависят от формата записи, используемого при записи данных в том. Можно принять стандартное значение для типа устройств или указать собственное значение.

Чтобы задать примерную емкость ленточных томов, используйте параметр **ESTCAPACITY** при создании или обновлении определения класса устройств.

Информация, связанная с данной

[DEFINE DEVCLASS \(Задать класс устройств\)](#)

[UPDATE DEVCLASS \(изменение класса устройства\)](#)

Указание формата записей для ленточных носителей

Можно задать формат записи, используемый IBM Spectrum Protect для записи данных на ленточный носитель. Если вы собираетесь использовать в библиотеке разные поколения накопителей или разные типы накопителей, вы должны задать формат записи для каждого поколения накопителей и для каждого типа накопителей. Тогда сервер сможет различать поколения накопителей и типы накопителей.

Об этой задаче

Чтобы задать формат записи, используйте параметр **FORMAT** при создании или обновлении определения класса устройств.

Если формат всех накопителей, связанных с этим классом устройства, одинаков, укажите **FORMAT=DRIVE**. На сервере выбирается самый высокий формат, поддерживаемый накопителем, на котором смонтирован том.

Если некоторые накопители, связанные с классом устройств, поддерживают формат более плотной записи, чем другие, и укажите формат, совместимый со всеми накопителями.

Если в одной библиотеке SCSI есть накопители, основанные на разных технологиях ленточных устройств (например, DLT и LTO Ultrium), задайте уникальное значение параметра **FORMAT** для каждого определения класса устройств.

Пример конфигурирования смотрите в разделе [Пример: конфигурирование библиотеки SCSI или виртуальной ленточной библиотеки с несколькими типами накопителей](#).

Формат записи, который сервер использует для тома, выбирается при первой записи данных на том. Обновление параметра **FORMAT** не влияет на носители, которые уже содержат информацию, до тех пор, пока эти носители не будут перезаписаны сначала. Этот процесс может происходить после того, как том освобожден или удален, или после того, как все данные на томе устареют.

Информация, связанная с данной

[DEFINE DEVCLASS \(Задать класс устройств\)](#)

[UPDATE DEVCLASS \(изменение класса устройства\)](#)

Как связать объекты библиотеки с классами устройств

Библиотека содержит накопители, которые можно использовать для монтирования тома. С классом устройства может быть связана только одна библиотека. Тем не менее, несколько классов устройств могут обращаться к одной библиотеке.

Об этой задаче

Чтобы связать класс устройств с библиотекой, используйте параметр **LIBRARY** при создании или обновлении определения класса устройств.

Информация, связанная с данной

[DEFINE DEVCLASS \(Задать класс устройств\)](#)

[UPDATE DEVCLASS \(изменение класса устройства\)](#)

Управление операциями монтирования носителей для ленточных и оптических устройств

Используя определения классов устройств, можно управлять числом смонтированных томов, интервалом времени, в течение которого том остается смонтированным, а также тем, сколько времени сервер IBM Spectrum Protect будет ждать, чтобы накопитель стал доступен.

Управление числом одновременно смонтированных томов

Задавая предел монтирования для класса устройств, вы должны учесть, сколько устройств хранения связано с вашей системой. Также следует учесть, используется ли функция одновременной записи, связываете ли вы несколько классов устройств с одной библиотекой, а также то, сколько процессов выполняются одновременно.

Об этой задаче

При выборе лимита монтирования класса устройств учтите следующее:

- Сколько устройств хранения подключено к вашей системе?

Не указывайте значение лимита монтирования, превышающее количество связанных доступных накопителей в вашей системе. Если сервер пытается смонтировать столько же томов, сколько задано лимитом монтирования, а больше для нужного тома нет доступных накопителей, происходит ошибка и сеанс клиента может быть завершен. (Это ограничение не относится к случаю, когда указан параметр **DRIVES**.)

Если у вас ресурсы библиотеки совместно используются в SAN разными серверами IBM Spectrum Protect, вы должны ограничить число ленточных накопителей, которые клиент библиотеки может использовать за один раз. Чтобы разрешить нескольким серверам клиентов библиотеки использовать библиотеку одновременно, задайте параметр **MOUNTLIMIT**, когда будете задавать или обновлять класс устройств на клиенте библиотеки. Дополнительную информацию о конфигурировании совместного использования библиотек смотрите в разделе [“Конфигурирование совместного использования библиотек”](#) на стр. 105.

- Используется ли функция одновременной записи в первичных пулах хранения, пулах хранения копий и пулах активных данных?

Задайте лимит монтирования, обеспечивающий достаточно точек монтирования для поддержки одновременной записи в первичный пул хранения и все связанные с ним пулы хранения копий и пулы активных данных.

- Связываете ли вы несколько классов устройств с одной библиотекой?

Класс устройства, связанный с библиотекой, может использовать любой накопитель из библиотеки, совместимый с классом и типом устройства. Поскольку с библиотекой можно связать несколько классов устройств, один накопитель в библиотеке может использоваться несколькими классами устройств. IBM Spectrum Protect гарантирует, что две операции не смогут одновременно использовать один и тот же накопитель, используя два разных класса устройств.

- Сколько процессов IBM Spectrum Protect необходимо запускать одновременно с использованием устройств этого класса?

IBM Spectrum Protect автоматически отменяет некоторые процессы, чтобы запустить другие, с более высоким приоритетом. Если на сервере задействованы все доступные накопители данного класса устройств для выполнения процессов с более высоким приоритетом, процессы с более низким приоритетом должны ожидать, пока накопитель не будет доступен. Например, IBM Spectrum Protect отменяет для клиента процесс, когда производится непосредственное резервное копирование на ленту, если накопитель нужен для процесса переноса сервера или освобождения ленты. IBM Spectrum Protect отменяет процесс освобождения ленты, если накопитель нужен для операции восстановления клиента. Дополнительную информацию смотрите в разделе [“Прерывание операций”](#) на стр. 135.

Если процессы часто отменяются другими процессами, возможно, следует сделать больше накопителей доступными для использования в IBM Spectrum Protect. Можно также изменить расписание операций, чтобы уменьшить нагрузку на накопители.

Это замечание также относится к функции одновременной записи. Чтобы обеспечить успешное выполнение операции одновременной записи, надо иметь достаточное число накопителей.

Чтобы задать максимальное число томов, которые можно одновременно смонтировать, используйте параметр **MOUNTLIMIT** при создании или обновлении определения класса устройств.

Информация, связанная с данной

[DEFINE DEVCLASS \(Задать класс устройств\)](#)

[UPDATE DEVCLASS \(изменение класса устройства\)](#)

Управление интервалом времени, в течение которого том остается смонтированным

Можно управлять интервалом времени, в течение которого смонтированный том останется смонтированным после выполнения последней операции ввода-вывода. Если том часто используется, можно улучшить его производительность, установив большую задержку размонтирования, чтобы избежать ненужных операций монтирования и размонтирования.

Об этой задаче

Если операции монтирования выполняются вручную оператором, вам, возможно, стоит задать большую задержку размонтирования. Например, если один оператор обслуживает систему в выходные дни, задайте большую задержку размонтирования, чтобы система не спрашивала оператора каждые несколько минут, следует ли монтировать тома.

Чтобы управлять интервалом времени, в течение которого смонтированный том останется смонтированным, используйте параметр **MOUNTRETENTION** при создании или обновлении определения класса устройств. Например, если значение задержки размонтирования равно 60 и смонтированный том простаивает в течение 60 минут, то сервер размонтирует том.

Если IBM Spectrum Protect монтирует том, накопитель выделяется для IBM Spectrum Protect и не может использоваться в других целях. Если требуется освободить накопитель для других целей, можно отменить операции IBM Spectrum Protect, в которых используется накопитель, а затем размонтировать том. Например, можно отменить операцию перенастройки сервера или резервного копирования. Информацию о том, как отменить процессы и размонтировать тома, смотрите в разделе [“Управление серверными запросами на тома”](#) на стр. 205.

Информация, связанная с данной

[DEFINE DEVCLASS \(Задать класс устройств\)](#)

[UPDATE DEVCLASS \(изменение класса устройства\)](#)

Управление временем ожидания накопителя сервером

Вы можете задать максимальное время (в минутах), в течение которого сервер IBM Spectrum Protect должен ждать, когда накопитель станет доступен для выполнения текущего запроса на монтирование.

Об этой задаче

Для управления временем ожидания доступности накопителя по запросу монтирования используйте параметр **MOUNTWAIT** при определении или изменении класса устройств.

Информация, связанная с данной

[DEFINE DEVCLASS \(Задать класс устройств\)](#)

[UPDATE DEVCLASS \(изменение класса устройства\)](#)

Прерывание операций

Сервер может прервать операции клиента или сервера для более приоритетной задачи, если точка монтирования используется, а других доступных точек нет, или если требуется доступ к конкретному тому. Когда операция прерывается, она отменяется.

Для просмотра состояния тома для точки монтирования, можно использовать команду **QUERY MOUNT**.

По умолчанию прерывание для сервера включено. Чтобы запретить прерывание, задайте опцию **NOPREEMPT** в файле опций сервера. Если вы зададите эту опцию, единственными операциями, которым разрешено прерывать другие операции, останутся команда **BACKUP DB** и команды экспорта и импорта.

Информация, связанная с данной

[BACKUP DB \(Выполнить резервное копирование базы данных\)](#)

[QUERY MOUNT \(Вывод сведений о смонтированных томах с последовательным доступом\)](#)

Приоритетное прерывание точки монтирования

Если для операции с высоким приоритетом требуется точка монтирования в конкретном классе устройства, а все точки монтирования в этом классе в настоящее время используются, операция с высоким приоритетом может перехватить точку монтирования у операции с низким приоритетом.

Точки монтирования могут быть перехвачены только в тех случаях, когда совпадает класс устройства у перехватывающей операции и у той операции, которая прерывается.

Следующие операции высокого приоритета могут прервать другие операции для доступа к точке монтирования.

- Операции резервного копирования базы данных
- Операции получения, восстановления или возврата HSM, инициированные клиентами
- Операции восстановления с использованием удаленного средства перемещения данных
- Операции экспорта
- Операции импорта
- Операции генерирования набора резервных копий

Следующие операции на сервере не могут прервать другие операции или сами быть прерванными:

- Аудит тома
- Восстановление данных из пула копий или активных данных
- Подготовка файла плана восстановления
- Сохранение данных с помощью удаленного переноса данных

Могут быть прерваны следующие операции, перечисленные в порядке приоритета, от наибольшего приоритета к наименьшему. Сервер выбирает для прерывания операции с наименьшим приоритетом, например, идентификацию дубликатов.

- Репликация узлов
- Резервное копирование данных в пул хранения копий
- Копирование активных данных в пул активных данных
- Перемещение данных в том пула хранения
- Перенос данных с диска на носитель с последовательным доступом
- Перенос данных с одного носителя с последовательным доступом на другой
- Операции резервного копирования, архивирования и переноса HSM, инициированные клиентами
- Освобождение томов в пуле хранения с последовательным доступом
- Обнаружить дубликаты

Приоритетное прерывание доступа к тому

Если для операции с высоким приоритетом требуется доступ к конкретному тому, а этот том в настоящее время используется, операция с высоким приоритетом может прервать операцию с низким приоритетом для этого тома.

Например, если для запроса на восстановление требуется доступ к тому, который занят операцией освобождения пространства, и накопитель доступен, операция освобождения прерывается.

Следующие операции с высоким приоритетом могут прервать операции для доступа к конкретному тому:

- Операции резервного копирования базы данных
- Операции получения, восстановления или возврата HSM, инициированные клиентами
- Операции восстановления с использованием удаленного средства перемещения данных
- Операции экспорта
- Операции импорта
- Операции генерирования набора резервных копий

Следующие операции не могут прервать другие операции или сами быть прерванными:

- Аудит тома
- Восстановление данных из пула копий или активных данных
- Подготовка плана восстановления
- Сохранение данных с помощью удаленного переноса данных

Могут быть прерваны следующие операции, перечисленные в порядке приоритета, от наибольшего приоритета к наименьшему. Сервер выбирает для прерывания операции с наименьшим приоритетом, например, идентификацию дубликатов.

- Репликация узлов
- Резервное копирование данных в пул хранения копий
- Копирование активных данных в пул активных данных
- Перемещение данных в том пула хранения
- Перенос данных с диска на носитель с последовательным доступом
- Перенос данных с одного носителя с последовательным доступом на другой
- Операции резервного копирования, архивирования и переноса HSM, инициированные клиентом
- Освобождение томов в пуле хранения с последовательным доступом
- Обнаружить дубликаты

Влияние изменений устройств в SAN

Среда SAN может сильно измениться из-за изменения устройств или кабелей. Динамический характер SAN данных может привести к ошибкам или непредвиденному поведению статических определений.

ID устройств, назначенные сетью хранения данных и известные серверу или агенту хранения, могут быть изменены из-за сбросов шины или других изменений среды. Например, сервер может распознать устройство X как *rmt0* (в AIX) на основе исходной спецификации пути на сервере и исходной конфигурации локальной сети. Однако некоторые события в SAN, например, добавление нового устройства Y, приводят к назначению *rmt1* устройству X. При попытке сервера получить доступ к устройству X с использованием *rmt0* либо доступ завершится неудачно, либо будет осуществлен доступ не к тому устройству назначения. Сервер попытается выполнить восстановление после внесения изменений в устройства в SAN, используя серийные номера устройств для подтверждения идентичности устройств, к которым он обращается.

При определении носителя или библиотеки у вас есть опция указания серийного номера для этого устройства. Если при определении устройства серийный номер не был указан, сервер получит его во время определения пути к устройству. В любом случае в базе данных сервера будет серийный номер устройства, который он сможет использовать для подтверждения идентичности устройства для операции.

При использовании накопителей и библиотек в сети SAN сервер пытается проверить, является ли используемое устройство нужным устройством. Сервер устанавливает связь с устройством с помощью имени устройства и указанного пути. Затем сервер запрашивает серийный номер устройства и сравнивает его с серийным номером устройства в базе данных.

Если серийный номер не совпадает, сервер начинает процесс поиска устройств в SAN, пытаясь найти устройство с совпадающим серийным номером. Если сервер находит устройство с нужным серийным номером, он исправляет определение пути в базе данных сервера, обновив имя устройства, указанное в пути. Сервер выдает сообщение с информацией об изменении, произведенном в устройстве. Затем сервер приступает к использованию устройства.

Чтобы определить, когда изменения устройства в SAN влияют на сервер IBM Spectrum Protect, можно отслеживать сообщения в журнале операций. С серийными номерами связаны следующие сообщения:

- ANR8952 — ANR8958;
- ANR8961 - ANR8968;
- ANR8974 - ANR8975.

Ограничения: Некоторые устройства не могут сообщить свои серийные номера прикладным программам, таким как сервер IBM Spectrum Protect. Если сервер не может получить серийный номер с устройства, сервер не сможет помочь системе восстановиться после изменения расположения устройства в SAN.

Вывод сведений об устройстве

Можно посмотреть сведения об устройствах, соединенных с сервером, используя утилиту информации об устройствах (tsmdlst).

Прежде чем начать

- Убедитесь, что у вас установлен API HBA (адаптер шины хоста). API HBA требуется, чтобы запустить утилиту информации об устройствах.
- Убедитесь, что у вас установлен и сконфигурирован драйвер ленточных устройств.

Процедура

1. В командной строке перейдите в подкаталог `server` каталога установки сервера, например, `C:\Program Files\Tivoli\TSM\server`.
2. Запустите исполняемый файл `tsmdlst.exe`.

Информация, связанная с данной

[QUERY SAN \(Запросить список устройств в сети хранения данных\)](#)
[tsmdlst \(Вывод информации об устройствах\)](#)

Носители с однократной записью и многократным чтением (WORM)

Носители с однократной записью и многократным чтением (Write-Once, Read-Many - WORM) помогают предотвратить случайное или намеренное удаление критически важных данных. Однако в IBM Spectrum Protect существует ряд ограничений и рекомендаций, которым нужно следовать при использовании носителей WORM.

С IBM Spectrum Protect можно использовать следующие типы носителей WORM:

- IBM 3592, все поддерживаемые поколения

- IBM LTO-3 и все поддерживаемые поколения
- HP LTO-3 и все поддерживаемые поколения
- Quantum LTO-3 и все поддерживаемые поколения
- Quantum SDLT 600, Quantum DLT V4 и Quantum DLT S4.
- StorageTek VolSafe;
- Sony AIT50 и AIT100;

Советы:

- Пул хранения может состоять либо из носителей WORM, либо из носителей RW, но не из носителей обоих типов.
- Чтобы не тратить напрасно ленту после выполнения операции восстановления или импорта, не используйте ленты WORM для операций резервного копирования или экспорта базы данных.

Накопители, поддерживающие WORM

Чтобы можно было использовать в библиотеке носители WORM, все накопители библиотеки должны поддерживать WORM. Монтирование не удастся, если картридж WORM будет смонтирован в накопитель для чтения и записи (RW).

Однако накопитель, поддерживающий WORM, можно использовать в качестве RW-накопителя, если установить для параметра WORM в классе устройства значение NO. Библиотека любого типа может содержать носители как WORM, так и RW, если во *всех* устройствах активирован WORM. Единственным исключением из этого правила являются библиотеки, подключенные к NAS, в которых использование ленточных носителей WORM невозможно.

Информация, связанная с данной

[DEFINE DEVCLASS \(Задать класс устройств\)](#)

[UPDATE DEVCLASS \(изменение класса устройства\)](#)

Активация носителей WORM

Тип носителей WORM определяет, нужно ли читать метку носителя при активации носителя.

Чейнджеры носителей библиотек не способны распознать разницу между стандартным ленточным носителем RW (чтение/запись) и следующими типами ленточных носителей WORM:

- VolSafe
- Sony AIT
- LTO
- SDLT
- DLT

Чтобы определить тип используемого носителя WORM, том необходимо загрузить в накопитель. Поэтому при регистрации томов WORM одного из этих типов нужно указывать опцию CHECKLABEL=YES в команде **CHECKIN LIBVOLUME**.

Библиотечные чейнджеры IBM 3592, которые поддерживают носители WORM, могут определять, является ли том носителем WORM, без загрузки тома в накопитель. Указывать CHECKLABEL=YES не нужно. Следует выяснить у поставщика оборудования, обеспечивают ли накопители и библиотеки 3592 необходимую поддержку.

Информация, связанная с данной

[CHECKIN LIBVOLUME \(регистрация тома хранения в библиотеке\)](#)

Ограничения, касающиеся носителей WORM

Использовать носители WORM с заранее присвоенной меткой в сочетании с классом устройств LTO или ECARTRIDGE нельзя.

Носители WORM нельзя использовать, если IBM Spectrum Protect задан как менеджер ключей шифрования накопителей для следующих накопителей:

- IBM LTO-5, LTO-6 и новее
- HP LTO-5, LTO-6 и новее
- Oracle StorageTek T10000B
- Oracle StorageTek T10000C
- Oracle StorageTek T10000D

Ошибки монтирования при использовании носителей класса WORM

Если ленточный носитель WORM загрузить в накопитель для устройств класса RW (чтение и запись), то монтирование завершится неудачно. Аналогичным образом, если ленточный носитель RW загрузить в накопитель для устройств класса WORM, то монтирование завершится неудачно.

Изменение меток носителей WORM

Если картридж WORM содержит данные, изменять его метку нельзя. Это касается картриджей Sony AIT WORM, LTO WORM, SDLT WORM, DLT WORM и IBM 3592. Метку на томе VolSafe можно перезаписать только один раз и только при условии, что том не содержит используемых, удаленных или просроченных данных.

Вводите команду **LABEL LIBVOLUME** для каждого тома VolSafe только по одному разу. Защиту от изменения метки можно установить с помощью параметра **OVERWRITE=NO** команды **LABEL LIBVOLUME**.

Информация, связанная с данной

[LABEL LIBVOLUME \(запись метки на том библиотеки\)](#)

Удаление закрытых томов WORM из библиотеки

Если над томом WORM совершаются действия (например, удаление промежутков между файлами), и сервер не отмечает том как заполненный, то этому тому возвращается состояние чистого. Если том WORM, не отмеченный как заполненный, удалить из пула хранения, то он останется закрытым. Чтобы удалить закрытый том WORM из библиотеки, необходимо выполнить команду **CHECKOUT LIBVOLUME**.

Информация, связанная с данной

[CHECKOUT LIBVOLUME \(исключение тома хранения из библиотеки\)](#)

Создание томов DLT WORM

Тома DLT WORM можно преобразовать из томов RW (чтение/запись).

Чтобы обеспечить поддержку носителей WORM при работе с накопителями SDLT-600, DLT-V4 или DLT-S4, можно обновить эти накопители с использованием программно-аппаратного обеспечения V30 или более поздней версии, которое можно приобрести у Quantum. Можно также использовать программное обеспечение DLTIce для преобразования неформатированных томов RW или пустых томов в тома WORM.

В библиотеках SCSI сервер IBM Spectrum Protect автоматически создает чистые тома DLT WORM, когда не может найти никаких чистых томов WORM в перечне библиотеки. Сервер преобразует доступные неформатированные или пустые чистые тома RW, а также пустые закрытые тома RW, в чистые тома WORM. Сервер также меняет метки на вновь созданных томах WORM, используя информацию из меток существующих томов RW.

Поддержка коротких и обычных лент 3592 WORM

IBM Spectrum Protect поддерживает как короткие, так и обычные ленты 3592 WORM. Для получения наилучших результатов их следует задавать в отдельных пулах хранения

Как запросить в классе устройств информацию о значении параметра WORM

Значение параметра WORM для класса устройств можно определить, введя команду **QUERY DEVCLASS**. Выходная информация будет содержать поле "WORM", в котором будет находиться значение YES (Да) или NO (Нет).

Информация, связанная с данной

Команда **QUERY DEVCLASS** (отображение информации об одном или нескольких классах устройств)

Устранение ошибок устройств

Можно произвести поиск и устранение ошибок, возникших при конфигурировании или использовании устройств с IBM Spectrum Protect.

Об этой задаче

Используйте Таблица 26 на стр. 140 для поиска решения возникшей с устройством проблемы.





Таблица 26. Устранение проблем устройств		
Симптом	Проблема	Решение
Конфликты с другими программами.	Продукту IBM Spectrum Protect требуется сеть хранения данных для совместного использования устройств.	Настроить сеть хранения данных.  Внимание: Если несколько серверов IBM Spectrum Protect используют одно и то же устройство, возможна потеря данных. Задавайте или используйте устройство только с одним сервером IBM Spectrum Protect   Другие приложения могут получить доступ к устройствам IBM Spectrum Protect, используя ленточный драйвер SCSI.
Ошибка присвоения метки.	Устройство для присвоения метки томам нельзя использовать во время использования сервером устройства для выполнения других процессов.	Перезаписать существующие тома в пуле хранения нельзя. Вы должны устранить все аппаратные ошибки, прежде чем присваивать тому метку.
	Неправильная или неполная регистрация лицензии.	Зарегистрируйте приобретенную лицензию на поддержку устройств.
Конфликты между драйверами устройств.	IBM Spectrum Protect выводит сообщения об ошибках ввода-вывода при определении или использовании устройств с последовательным доступом.	 Драйверы устройств Windows и драйверы, предоставляемые другими прикладными программами, могут конфликтовать с драйвером устройств IBM Spectrum Protect, если драйвер IBM Spectrum Protect не запущен первым. Чтобы проверить порядок запуска драйверов устройств системой, выполните следующие шаги: 1. Щелкните по значку Панель управления . 2. Щелкните по Устройства . Драйвера устройств и соответствующие типы запуска перечислены.
Ошибки ввода-вывода	Если вы попытаетесь задать или использовать ленточное устройство, могут возникнуть конфликты драйверов устройств. Драйверы устройств Windows и драйверы, предоставляемые другими прикладными программами, могут конфликтовать с драйвером устройств IBM Spectrum Protect, если он не запущен первым.	

Таблица 26. Устранение проблем устройств (продолжение)

Симптом	Проблема	Решение
<p>Linux Не удается предупредить конфликт резервирования ленточных накопителей с постоянным резервом на платформе Linux.</p>	<p>Linux На платформе Linux серверу или агенту хранения IBM Spectrum Protect требуется, чтобы был сконфигурирован драйвер устройств IBM lin_tape для постоянного резерва и был создан файл псевдоустройства IBM /dev/TSMtape.</p>	<p>Linux Если для драйвера IBM lin_tape включена отказоустойчивость пути данных, автоматически создается файл /dev/TSMtape и можно использовать постоянный резерв. Либо сконфигурируйте постоянный резерв для резервирования ленточных накопителей на платформе Linux в соответствии со следующей процедурой:</p> <p>Совет: По умолчанию драйвер устройств IBM lin_tape использует резерв SCSI-2 для резервирования ленточных накопителей.</p> <p>Linux</p> <ol style="list-style-type: none"> 1. Разгрузите драйвер устройства IBM lin_tape. 2. В файле конфигурации lin_tape /etc/modprobe.conf или /etc/modprobe.conf.local (или, если вы работаете в RHEL 6 или выше, /etc/modprobe.d/lin_tape.conf), добавьте следующую строку: <pre>options lin_tape tape_reserve_type=persistent</pre> 3. В файле правил /etc/udev/rules.d/98-lin_tape.rules добавьте следующую строку: <pre>KERNEL=="TSMtape", MODE=="0666"</pre> 4. Перезагрузите драйвер устройства IBM lin_tape. <p>Linux Будет создан псевдо-файл IBM, /dev/TSMtape, и сервер IBM Spectrum Protect сможет использовать постоянный резерв для предупредительного резервирования ленточных накопителей на платформах Linux.</p>

Завершение реализации

После того, как решение IBM Spectrum Protect будет сконфигурировано и заработает, проверьте операции резервного копирования и настройте мониторинг, чтобы убедиться, что все нормально работает.

Процедура

1. Проверьте операции резервного копирования, чтобы убедиться, что ваши данные защищены, как вы и ожидали.
 - a) Выберите на странице **Клиенты** компонента Центр операций клиенты, для которых вы хотите выполнить резервное копирование, и щелкните по **Резервное копирование**.
 - b) На странице **Серверы** в компоненте Центр операций выберите сервер, для которого вы хотите производить резервное копирование базы данных. Щелкните по **Резервное копирование** и выполните инструкции в окне **Резервное копирование базы данных**.
 - c) Убедитесь, что резервное копирование выполнено без предупреждений или сообщений об ошибках.

Совет: Либо можно использовать графический интерфейс клиента резервного копирования и архивирования для резервного копирования данных клиента, и можно производить

резервное копирование базы данных, вводя команду **BACKUP DB** из административной командной строки.

2. Настройте мониторинг для ваших решений, следуя инструкциям в разделе [Часть 3, “Мониторинг решения на лентах”, на стр. 143.](#)

Часть 3. Мониторинг решения на лентах

Отслеживайте свое основанное на ленте решение, чтобы гарантировать правильную работу.

Об этой задаче

После реализации ленточного решения IBM Spectrum Protect с несколькими площадками отслеживайте решение ежедневно и периодически, чтобы выявлять существующие и потенциальные проблемы. Собранную вами информацию можно использовать, чтобы устранять проблемы и оптимизировать производительность системы. Предпочтительный способ мониторинга решения заключается в использовании компонента Центр операций, который позволяет получить общее и подробное состояние системы в графическом пользовательском интерфейсе. Кроме того, можно сконфигурировать Центр операций для генерирования отчетов по электронной почте, в которых суммируется состояние системы.

Процедура

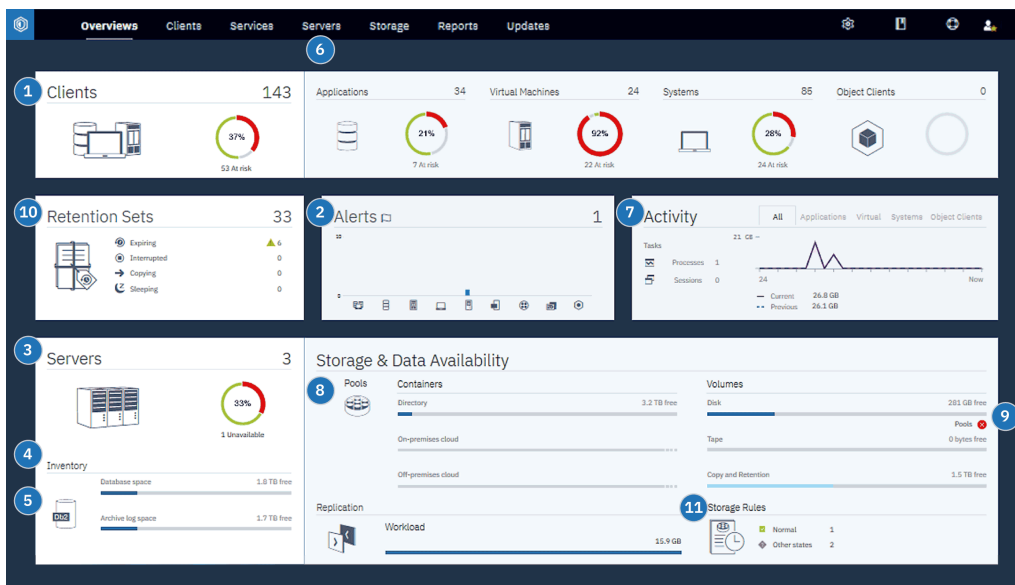
1. Выполните задачи ежедневного мониторинга. Инструкции смотрите в разделе [Контрольный список ежедневного мониторинга](#).
2. Выполните задачи периодического мониторинга. Инструкции смотрите в разделе [Контрольный список периодического мониторинга](#).
3. Убедитесь, что ваша система удовлетворяет требованиям лицензирования. Инструкции смотрите в разделе [Проверка соответствия лицензии](#).
4. Необязательно: Настройте отчеты по электронной почте с информацией о состоянии системы. Инструкции смотрите в разделе [“Состояние системы отслеживания с использованием отчетов по электронной почте”](#) на стр. 165.


Контрольный список ежедневного мониторинга

Чтобы убедиться, что вы выполняете ежедневные задачи мониторинга для своего решения IBM Spectrum Protect, ознакомьтесь с ежедневным контрольным списком для мониторинга.

Выполняйте ежедневные задачи мониторинга со страницы **Обзор** в компоненте Центр операций. Доступ к странице **Обзор** можно получить, открыв Центр операций и щелкнув по **Обзоры**.

На рисунке ниже показано расположение для завершения каждой операции.



Совет: Чтобы выполнять команды администрирования для дополнительных задач по мониторингу, используйте построитель команд компонента Центр операций. Пстроитель команд обеспечивает функцию ввода с опережением, которая поможет по мере ввода команд. Чтобы открыть построитель команд, перейдите на страницу **Обзор** в компоненте Центр операций. В строке меню установите указатель мыши на значок параметров  и щелкните по **Построитель команд**.

В следующей таблице перечислены ежедневные задачи мониторинга и представлены инструкции по выполнению каждой задачи.

Таблица 27. Задачи ежедневного мониторинга

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
<p>Наблюдайте за уведомлениями о защите, которые могут указывать на атаку программы-вымогателя.</p>	<p>Если потенциальная атака программы-вымогателя обнаружена в среде IBM Spectrum Protect, то будет показано уведомление о защите на переднем плане Центра операций. Дополнительную информацию можно получить, щелкнув по сообщению, чтобы открыть страницу Уведомления о защите.</p>	<p>На странице Уведомления о защите можно выполнить следующие действия:</p> <ul style="list-style-type: none"> • Просмотр подробностей уведомления по клиентам. <p>Ограничение: Уведомления доступны только для клиентов резервного копирования и архивирования и для клиентов IBM Spectrum Protect for Virtual Environments.</p> <ul style="list-style-type: none"> • Подтвердите уведомление защиты, выбрав его и щелкнув по Подтвердить. При подтверждении уведомления о защите в столбец Подтверждение на странице Уведомления о защите добавляется символ галочки для выбранного клиента. Стандарт, по которому подтверждается уведомление, определяется в вашей организации. Галочка может означать, что вы исследовали проблему и решили, что это - ложное положительное. Это также может означать, что проблема существует, и она решается. • Назначьте уведомление о защите администратору, выбрав уведомление о защите и нажав Назначить. Чтобы рассмотреть назначение, администратор должен зарегистрироваться в Центре операций и щелкнуть Обзоры > Защита. Если вы не уверены, что администратор регулярно отслеживает страницу Уведомления о защите, сообщите администратору о назначении. • Если уведомление - ложное положительное, то можно выбрать уведомление о защите и щелкните по Сброс. Уведомление о защите удалено. Хронологические данные, используемые для базовых сравнений с самой последней операцией резервного копирования, удаляются. С этого момента вычисляется новая базовая линия. • (Необязательно) Можно отключить уведомления защиты с помощью команды SET SECURITYNOTIF.

Таблица 27. Задачи ежедневного мониторинга (продолжение)


Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
<p>1 Определите, подвергаются ли клиенты риску оказаться незащищенными из-за неудавшихся или пропущенных операций резервного копирования.</p>	<p>Чтобы проверить, находятся ли клиенты под угрозой, в области Клиенты найдите уведомление Под угрозой. Чтобы просмотреть сведения, щелкните по области Клиенты.</p> <p> Внимание: Если процент Под угрозой намного больше обычного, то это может указывать на атаку программы-вымогателя. Атака программы-вымогателя может привести к сбоям резервного копирования, тем самым создавая риск для клиентов. Например, если процент клиентов в опасности обычно между 5% и 10%, но процент увеличивается до 40% или 50%, то изучите причину этого.</p> <p>Если вы установили службу управления клиентом на клиенте резервного копирования и архивирования, вы сможете увидеть и проанализировать ошибку клиента и запланировать журналы, выполнив следующие шаги:</p> <ol style="list-style-type: none"> 1. В таблице Клиенты выберите клиент и щелкните по Сведения. 2. Чтобы диагностировать проблему, щелкните по Диагноз. 	<p>В случае клиентов, у которых нет установленной службы управления клиентом, получите доступ к системе клиента, чтобы проверить журналы ошибок клиента.</p>
<p>2 Определите, нужно ли уделить внимание ошибкам клиента или сервера.</p>	<p>Чтобы определить серьезность всех оповещений, о которых было сообщено, установите указатель мыши на столбцы в области Оповещения.</p>	<p>Чтобы увидеть дополнительную информацию об оповещениях, выполните следующие шаги:</p> <ol style="list-style-type: none"> 1. Щелкните по области Оповещения. 2. В таблице Оповещения выберите оповещение. 3. В панели Журнал операций просмотрите сообщения. В панели показаны связанные сообщения, созданные до и после возникновения выбранного оповещения.

Таблица 27. Задачи ежедневного мониторинга (продолжение)

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
<p>3 Определите, доступны ли серверы, которыми управляет Центром операций, для предоставления клиентам служб по защите данных.</p>	<ol style="list-style-type: none"> 1. Чтобы проверить, находятся ли серверы под угрозой, в области Серверы найдите уведомление Недоступен. 2. Чтобы увидеть дополнительную информацию, щелкните по области Серверы. 3. Выберите сервер в таблице Серверы и щелкните по Сведения. 	<p>Совет: Если вы обнаружите проблему, связанную со свойствами сервера, обновите свойства сервера:</p> <ol style="list-style-type: none"> 1. В таблице Серверы выберите сервер и щелкните по Сведения. 2. Чтобы обновить свойства сервера, щелкните по Свойства.

Таблица 27. Задачи ежедневного мониторинга (продолжение)






Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
<p>4 Определите, доступно ли достаточно пространства для перечня сервера, состоящего из базы данных сервера, активного журнала и архивного журнала.</p>	<ol style="list-style-type: none"> Щелкните по области Серверы. В столбце Состояние в таблице проверьте состояние сервера и устраните все ошибки: <ul style="list-style-type: none"> Нормальное  Для базы данных сервера, активного журнала и архивного журнала доступен достаточный объем пространства. Критическое  Для базы данных сервера, активного журнала или архивного журнала недостаточно пространства. Нужно немедленно добавить пространство, иначе работа служб защиты данных, предоставляемых сервером, будет прервана. Предупреждение  В базе данных сервера, активном журнале или архивном журнале заканчивается пространство. Если это условие повторяется, то нужно добавить пространство. Недоступно  Невозможно получить состояние. Убедитесь, что сервер работает и что в сети нет ошибок. Это состояние показывается также, если ID администратора мониторинга заблокирован или недоступен на сервере по другой причине. Значение этого ID - IBM-ОС-имя_хаб-сервера. Неотслеживаемый  Неотслеживаемые серверы заданы на хаб-сервере, но не сконфигурированы для управления компонентом Центр операций. Чтобы сконфигурировать не отслеживаемый сервер, выберите сервер и щелкните по Отслеживать подчиненный. 	<p>Можно также просмотреть связанные оповещения на странице Оповещения. Дополнительную информацию об устранении ошибок смотрите в разделе <u>Устранение проблем сервера</u>.</p>

Таблица 27. Задачи ежедневного мониторинга (продолжение)


Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
<p>5 Проверьте операции резервного копирования базы данных.</p>	<p>Чтобы определить, когда в последний раз производилось резервное копирование сервера, выполните следующие шаги:</p> <ol style="list-style-type: none"> 1. Щелкните по области Серверы. 2. В таблице Серверы проверьте столбец Последнее резервное копирование базы данных. 	<p>Чтобы получить более подробную информацию об операциях резервного копирования, выполните следующие шаги:</p> <ol style="list-style-type: none"> 1. В таблице Серверы выберите строку и щелкните по Сведения. 2. В области Резервное копирование БД установите указатель мыши на галочки, чтобы прочесть информацию об операциях резервного копирования. <p>Если резервное копирование базы данных не производилось недавно (например, за последние 24 часа), вы можете запустить операцию резервного копирования:</p> <ol style="list-style-type: none"> 1. На странице Обзор в компоненте Центр операций щелкните по области Серверы. 2. В таблице выберите сервер и щелкните по Резервное копирование. <p>Чтобы определить, сконфигурирована ли база данных сервера для автоматических операций резервного копирования, выполните следующие шаги:</p> <ol style="list-style-type: none"> 1. В строке меню установите указатель мыши на значок параметров  и щелкните по Построитель команд. 2. Введите команду QUERY DB: <pre>query db f=d</pre> <ol style="list-style-type: none"> 3. В выходной информации проверьте значение в поле Полное имя класса устройств. Если класс устройства указан, это означает, что сервер сконфигурирован для автоматического резервного копирования базы данных.

Таблица 27. Задачи ежедневного мониторинга (продолжение)


Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
<p>6 Отслеживайте другие задачи по обслуживанию сервера. Задачи по обслуживанию сервера могут включать в себя выполнение расписаний административных команд, сценариев обслуживания и связанных команды.</p>	<p>Чтобы найти информацию о процессах, которые завершились неудачно из-за проблем на сервере, выполните следующие шаги:</p> <ol style="list-style-type: none"> 1. Выберите Серверы > Обслуживание. 2. Чтобы получить двухнедельную хронологию процесса, смотрите столбец Хронология. 3. Чтобы получить больше информации о запланированном процессе, установите указатель мыши на переключателе, связанном с процессом. 	<p>Более подробную информацию о процессах мониторинга и устранении проблем смотрите в электронной справке компонента Центр операций.</p>
<p>7 Убедиться, что объем данных, переданных на серверы и полученных с них, находится в ожидаемом диапазоне.</p>	<ul style="list-style-type: none"> • Чтобы получить обзор операций за последние 24 часа, смотрите область Операции. • Чтобы сравнить активность за последние 24 часа с активностью за предыдущие 24 часа, смотрите показатели в областях Текущие и Предыдущие. 	<ul style="list-style-type: none"> • Если на сервер было отправлено больше данных, чем вы ожидали, определите, какие клиенты создают резервные копии большего объема данных, и исследуйте причину. Возможно, что дедупликация данных на стороне клиента работает неправильно. <p> Внимание: Если объем резервных данных значительно больше обычного, то это может указывать на атаку программы-вымогателя. Когда программа-вымогатель шифрует данные, система обнаруживает, что данные изменяются и что резервная копия создается для измененных данных. Тем самым тома резервного копирования становятся больше. Чтобы узнать, какие клиенты затронуты, выберите вкладку Приложения, Виртуальные машины или Системы.</p> <ul style="list-style-type: none"> • Если на сервер было отправлено меньше данных, чем вы ожидали, выясните, выполняются ли операции резервного копирования клиентов по расписанию.

Таблица 27. Задачи ежедневного мониторинга (продолжение)




Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
<p>8 Убедитесь, что пулы хранения доступны для резервного копирования данных клиента.</p>	<p>1. Если в области Хранение и доступность данных указаны проблемы, щелкните по Пулы, чтобы ознакомиться со сведениями:</p> <ul style="list-style-type: none"> Если показано состояние Критическое , это указывает на то, что в пуле хранения недостаточно доступного пространства или его состояние доступа - Недоступно. <p> Внимание: Если состояние критическое, то изучите причину:</p> <ul style="list-style-type: none"> Если скорость дедупликации данных в пуле хранения значительно снижается, то это может указывать на атаку программы-вымогателя. Во время атаки программы-вымогателя данные шифруются и не могут дедуплицироваться. Чтобы проверить скорость дедупликации данных, в таблице Пулы хранения проверьте значение в столбце Процент экономии. Если пул хранения неожиданно становится использован 100%, то это может указывать на атаку программы-вымогателя. Для проверки использования просмотрите значение в столбце Использованная емкость. Наведите мышь на значения, чтобы увидеть процент использованного и свободного пространства. <ul style="list-style-type: none"> Если показано состояние Предупреждение , в пуле хранения заканчивается 	<p>Чтобы увидеть емкость пула хранения, используемую за последние две недели, выберите строку в таблице Пулы хранения данных и щелкните по Сведения.</p> <p>Часть 3. Мониторинг решения на лентах 151</p>

Таблица 27. Задачи ежедневного мониторинга (продолжение)



Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
<p>9 Убедитесь, что устройства хранения доступны для операций резервного копирования.</p>	<p>В области Хранение и доступность данных, в разделе Тома под столбцами емкости проверьте состояние, показанное рядом с элементом Устройства. Если для любого устройства показано состояние Критическое  или Предупреждение , исследуйте проблему. Чтобы просмотреть сведения, щелкните по Устройства.</p>	<p>Ленточные устройства могут находиться в состоянии предупреждения или в критическом состоянии, если накопители недоступны. Диск недоступен, если он отключен, перестал отвечать серверу или если его путь отключен. Ленточное устройство может также находиться в критическом состоянии, если библиотека отключена. В других столбцах таблицы Ленточные устройства показано состояние роботизации библиотеки, накопителей и путей.</p> <p>Чтобы устранить проблемы с ленточными устройствами, находящимися в критическом состоянии, можно перевести накопитель в отключенное состояние, если вы хотите использовать его для других операций, например, для обслуживания. Чтобы перевести накопитель в отключенное состояние, выполните следующие шаги:</p> <ol style="list-style-type: none"> 1. На странице компонента Центр операций Хранение выберите Ленточные устройства. 2. Чтобы увидеть больше информации о ленточной библиотеке, выберите строку и щелкните по Сведения. 3. Чтобы перевести накопитель в отключенное состояние, выберите ленточный накопитель и щелкните по Отключено. <p>В случае операций резервного копирования лент убедитесь, что доступно достаточное число чистых лент. Если вы не уверены, есть ли у вас достаточное число доступных чистых лент, откройте записную книжку с подробной информацией, чтобы узнать об использовании ленты и увидеть оценку доступности чистых лент. Чтобы открыть записную книжку с подробной информацией, выберите библиотеку в таблице и щелкните по Сведения.</p>

Таблица 27. Задачи ежедневного мониторинга (продолжение)






Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
<p>10 Мониторинг наборов хранения.</p>	<p>Чтобы получить общее состояние наборов хранения, просмотрите область Наборы хранения на странице Центр операций Обзор:</p> <ul style="list-style-type: none"> В поле Выполнено указано число наборов хранения, созданных в базе данных сервера и отслеживаемых в перечне сервера. В поле Срок действия истек указывается число наборов хранения, для которых истек срок хранения данных. В поле Удалено указывается число наборов хранения, которые были удалены. <p>Чтобы просмотреть или изменить правила хранения, выберите Службы > Правила хранения.</p>	<p>Чтобы получить дополнительную информацию о наборах хранения, щелкните по области Наборы хранения, чтобы открыть страницу Наборы хранения. Чтобы просмотреть или изменить свойства набора хранения, дважды щелкните по набору хранения.</p> <p>Более подробную информацию можно получить, выполнив связанные команды:</p> <ol style="list-style-type: none"> На странице Обзор компонента Центр операций установите указатель мыши на значок параметров  и щелкните по Построитель команд. Чтобы узнать, какие задания создания набора хранения выполняются, прерваны или завершены, выполните команду QUERY JOB. Инструкции смотрите в разделе QUERY JOB (Запросить задание создания набора хранения). Чтобы запросить правила хранения, введите команду QUERY RETRULE. Инструкции смотрите в разделе QUERY RETRULE (запрос правила хранения). Чтобы запросить наборы хранения, введите команду QUERY RETSET. Инструкции смотрите в разделе QUERY RETSET (запрос набора хранения). Чтобы запросить содержимое набора хранения, введите команду QUERY RETSETCONTENTS. Инструкции смотрите в разделе QUERY RETSETCONTENTS (запрос содержимого набора хранения).

Таблица 27. Задачи ежедневного мониторинга (продолжение)

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
<p>11 Отслеживать правила хранения.</p>	<p>Чтобы получить общее состояние операций правил хранения, просмотрите область Правила хранения на странице Центр операций Обзор.</p>	<p>В сводке состояний выводятся самые недавние результаты обработки для правил хранения. Выводится число правил хранения в каждом из следующих состояний:</p> <ul style="list-style-type: none"> <p> Нормальное Число правил хранения, выполненных без ошибок.</p> <p> Предупреждение Число правил хранения, завершивших обработку, но переместивших или скопировавших не все подлежащие обработке данные. Некоторые файлы были пропущены, было достигнуто ограничение по времени для правила или же процесс был отменен.</p> <p> Неудачно Число правил хранения, не завершивших обработку. Например, возможно, серверу не удастся обработать данные из-за нехватки места в пуле хранения назначения или сервер не может получить доступ к пулу хранения.</p> <p> Другие состояния Число правил хранения в других состояниях. Сервер, на котором определено правило хранения, может оказаться недоступным для предоставления данных, либо может быть запущена более ранняя версия IBM Spectrum Protect, не поддерживающая состояние. Состояние может оказаться неприменимым, поскольку правило хранения не активировано или не выполняется.</p> <p>Совет: Значок выводится, только если одно или несколько правил хранения находятся в соответствующем состоянии. Для просмотра более подробной информации о каждом правиле хранения выберите Правила хранения, чтобы открыть страницу Правила хранения.</p>

Контрольный список периодического мониторинга

Чтобы убедиться, что операции осуществляются правильно, выполните задачи в периодическом контрольном списке мониторинга. Запланируйте периодические задачи достаточно часто, чтобы вы могли обнаружить потенциальные неполадки, прежде чем они вызовут проблемы.


Совет: Чтобы выполнять команды администрирования для дополнительных задач по мониторингу, используйте построитель команд компонента Центр операций. Построитель команд обеспечивает функцию ввода с опережением, которая поможет по мере ввода команд. Чтобы открыть построитель команд, перейдите на страницу **Обзор** в компоненте Центр операций. В строке меню установите указатель мыши на значок параметров  и щелкните по **Построитель команд**.

Таблица 28. Задачи периодического мониторинга

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
<p>Отслеживайте производительность системы.</p>	<p>Определите, сколько времени требуется для операций резервного копирования клиента:</p> <ol style="list-style-type: none"> Щелкните на странице Обзор в компоненте Центр операций по Клиенты. Найдите сервер, связанный с клиентом. Щелкните по Серверы. Выберите сервер и щелкните по Сведения. Чтобы увидеть продолжительность выполненных задач за последние 24 часа, щелкните по Выполненные задачи. Чтобы увидеть продолжительность задач, выполненных более 24 часов тому назад, используйте команду QUERY ACTLOG. Информацию об этой команде смотрите в разделе QUERY ACTLOG (Запросить информацию журнала операций). Если длительность операций резервного копирования клиента увеличивается при неясных причинах, исследуйте причину. <p>Если вы установили службу управления клиентом на клиенте резервного копирования и архивирования, вы сможете диагностировать ошибки, влияющие на производительность, для клиента резервного копирования и архивирования, выполнив следующие шаги:</p> <ol style="list-style-type: none"> Щелкните на странице Обзор в компоненте Центр операций по Клиенты. Выберите клиент резервного копирования и архивирования и щелкните по Сведения. Чтобы получить журналы клиентов, щелкните по Диагностика. 	<p>Ограничьте время для операций резервного копирования клиента 8-12 часами. Убедитесь, что расписания клиентов не перекрываются с задачами по обслуживанию сервера.</p> <p>Инструкции по сокращению времени, которое затрачивает клиент на резервное копирование данных на сервер, смотрите в разделе https://www.ibm.com/support/knowledgecenter/en/SSEQVQ_8.1.0/perf/c_bac_perf_opts.html.</p> <p>Ищите узкие места с точки зрения производительности. Инструкции смотрите в разделе Определение узких мест производительности.</p> <p>Информацию о выявлении и устранении других проблем, отрицательно влияющих на производительность, смотрите в разделе https://www.ibm.com/support/knowledgecenter/en/SSEQVQ_8.1.0/perf/c_performance.html.</p>

Таблица 28. Задачи периодического мониторинга (продолжение)

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
<p>Убедитесь, что текущие файлы резервных копий для конфигурации устройств и информации о хронологии томов сохранены.</p>	<p>Получите доступ к расположениям хранения, чтобы убедиться, что файлы доступны. Предпочтительный метод заключается в том, чтобы сохранять файлы резервных копий в двум расположениях.</p> <p>Чтобы найти файлы хронологии томов и файлы конфигурации устройств, выполните следующие шаги:</p> <ol style="list-style-type: none"> 1. На странице Обзор Центра операций установите указатель мыши на значок параметров и щелкните по Построитель команд. 2. Чтобы найти файлы хронологии томов и конфигурации устройств, введите следующие команды: <div data-bbox="532 989 906 1045" data-label="Text"> <pre>query option volhistory</pre> </div> <div data-bbox="532 1058 906 1115" data-label="Text"> <pre>query option devconfig</pre> </div> 3. В выходной информации проверьте столбец Параметр опции, чтобы найти расположения файлов. <p>Если произойдет бедствие, для восстановления базы данных сервера потребуется как файл хронологии томов, так и файл конфигурации устройств.</p>	

Таблица 28. Задачи периодического мониторинга (продолжение)

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
<p>Определите, доступно ли достаточно пространства в каталоге для экземпляра сервера.</p>	<p>Убедитесь, что в каталоге для экземпляра сервера доступно хотя бы 50 ГБ свободного пространства. Выполните действие, подходящее для вашей операционной системы:</p> <ul style="list-style-type: none"> AIX Чтобы увидеть, сколько пространства доступно в файловой системе, введите в командной строке операционной системы следующую команду: <pre>df -g каталог_экземпляра</pre> <p>где <i>каталог_экземпляра</i> - это каталог экземпляра.</p> Linux Чтобы увидеть, сколько пространства доступно в файловой системе, введите в командной строке операционной системы следующую команду: <pre>df -h каталог_экземпляра</pre> <p>где <i>каталог_экземпляра</i> - это каталог экземпляра.</p> Windows В проводнике Windows щелкните правой кнопкой мыши по файловой системе и выберите Свойства. Проверьте информацию о емкости. <p>Предпочтительное расположение каталога экземпляра зависит от операционной системы, в которой установлен сервер:</p> <ul style="list-style-type: none"> Linux AIX /home/tsminst1/tsminst1 Windows C:\tsminst1 <p>Совет: Если вы заполнили рабочую таблицу планирования, расположение каталога экземпляров записано в рабочей таблице.</p>	

Таблица 28. Задачи периодического мониторинга (продолжение)

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
<p>Выявите неожиданную активность клиента.</p>	<p>Чтобы отслеживать операции клиента и определить, не превышает ли объем данных для томов ожидаемый объем, выполните следующие шаги:</p> <ol style="list-style-type: none"> 1. На странице Обзор в компоненте Центр операций щелкните по области Клиенты. 2. Чтобы увидеть операции за последние две недели, дважды щелкните по любому клиенту. 3. Чтобы узнать число байт, отправленных клиенту, щелкните по вкладке Свойства. 4. В области Последний сеанс проверьте строку Отправлено клиенту. 	<p>Когда вы дважды щелкнете по клиенту в таблице Клиенты, в области Операции за 2 недели будет показан объем данных, которые клиент каждый день отправлял на сервер.</p> <p>Регулярно проверяйте SQL-таблицу сводной информации о деятельности, содержащую статистические данные о клиентских сеансах. Чтобы сравнить текущие операции с предыдущими, воспользуйтесь оператором SQL SELECT. Если уровень операций существенно отличается от предыдущего, то это может указывать на атаку программы-вымогателя.</p> <p>Регулярно проверяйте журнал операций. Найдите сообщения ANE, указывающие, для скольких файлов созданы резервные копии и выполнена инспекция. Сравните текущие данные о скорости дедупликации с прежней скоростью. Если в созданной резервной копии необычно много файлов или уровень дедупликации данных неожиданно спадает до 0, то это может указывать на атаку программы-вымогателя</p>

Таблица 28. Задачи периодического мониторинга (продолжение)

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Отслеживайте рост пула хранения с течением времени.	<ol style="list-style-type: none"> 1. На странице Обзор в компоненте Центр операций щелкните по области Пулы. 2. Чтобы увидеть емкость, используемую за последние две недели, выберите пул и щелкните по Сведения. 	<p>Советы:</p> <ul style="list-style-type: none"> • Чтобы задать период времени, который должен пройти, прежде чем из пула хранения каталогов-контейнеров или пула хранения облачных контейнеров будут удалены все дедуплицированные экстененты, после того как на них не появлялось никаких ссылок в перечне, выполните следующие шаги: <ol style="list-style-type: none"> 1. На странице Пулы хранения в компоненте Центр операций выберите пул хранения. 2. Выберите Сведения > Свойства. 3. Задайте длительность в поле Период задержки для повторного использования контейнера. • Чтобы определить производительность дедупликации данных для пулов хранения каталогов-контейнеров и облачных контейнеров, используйте команду GENERATE DEDUPSTATS. • Чтобы просмотреть статистику дедупликации данных для пула хранения, выполните следующие шаги: <ol style="list-style-type: none"> 1. На странице Пулы хранения в компоненте Центр операций выберите пул хранения. 2. Выберите Сведения > Свойства. <p>Либо используйте команду QUERY EXTENTUPDATES, чтобы увидеть информацию об обновлениях экстенентов данных в пулах хранения каталогов-контейнеров или облачных контейнеров. Выходная информация команды может помочь вам определить, на какие экстененты данных уже нет ссылок и какие из них подлежат удалению из системы. В выходной информации смотрите, какое число экстенентов данных подлежит удалению из системы. Этот показатель напрямую коррелируется с объемом свободного пространства, которое доступно в пуле хранения контейнера.</p> • Чтобы увидеть объем физического пространства, занятого файловым пространством после удаления экономии за счет дедупликации данных, используйте команду select * from occupancy. В выходной информации команды будет содержаться значение LOGICAL_MB. LOGICAL_MB - это объем, используемый этим файловым пространством.

Таблица 28. Задачи периодического мониторинга (продолжение)

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Отслеживайте и обслуживайте ленточные устройства.	<p>Отслеживайте в своей среде аппаратные ошибки на ленточных устройствах и ленточных библиотеках. Инструкции смотрите в разделе “Мониторинг оповещений ленточных устройств для выявления аппаратных ошибок” на стр. 162.</p> <p>Отслеживайте совместимость носителей для предотвращения ошибок на ленточных устройствах. Инструкции смотрите в разделе “Как избежать ошибок, связанных с несовместимостью носителей” на стр. 163.</p> <p>Следите за сообщениями об очистке для ленточных накопителей. Инструкции смотрите в разделе “Операции с чистящими картриджами” на стр. 163.</p>	
Оцените временные характеристики расписаний клиента. Убедитесь, что начальное и конечное время расписаний клиента не перекрывает задачи по обслуживанию сервера. Ограничьте время для операций резервного копирования клиента 8-12 часами.	<p>На странице Обзор Центра операций щелкните по Клиенты > Расписания.</p> <p>В таблице Расписания в столбце Запуск показано сконфигурированное время запуска для запланированной операции. Чтобы увидеть, когда была запущена самая последняя операция, установите указатель мыши на значок часов.</p>	<p>Совет: Если операция клиента выполняется дольше, чем ожидается, вы можете получить сообщение с предупреждением. Сделайте следующее:</p> <ol style="list-style-type: none"> 1. На странице обзора в компоненте Центр операций установите указатель мыши на Клиенты и щелкните по Расписания. 2. Выберите расписание и щелкните по Сведения. 3. Просмотрите сведения о расписании, щелкнув по синей стрелке рядом со строкой. 4. В поле Оповещение среды выполнения задайте время, когда будет выдано сообщение с предупреждением, если запланированная операция не будет выполнена. 5. Щелкните по Сохранить.

Таблица 28. Задачи периодического мониторинга (продолжение)		
Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Оцените временные характеристики задач по обслуживанию. Убедитесь, что начальное и конечное время задач по обслуживанию не накладывается на расписания клиентов.	На странице Обзор Центра операций щелкните по Серверы > Обслуживание . В таблице Обслуживание проверьте информацию в столбце Время последнего выполнения. Чтобы увидеть, когда была запущена самая последняя задача по обслуживанию, установите указатель мыши на значок часов.	Предпочтительный метод заключается в том, что каждая задача по обслуживанию выполняется до ее завершения, прежде чем запустится следующая задача по обслуживанию. Примерами задач по обслуживанию являются признание перечня устаревшим, копирование пулов хранения, освобождение пространства и резервное копирование базы данных. Совет: Если задача по обслуживанию выполняется слишком долго, измените начальное время или максимальное время работы. Сделайте следующее: 1. На странице Обзор Центра операций установите указатель мыши на значок параметров и щелкните по Построитель команд . 2. Чтобы изменить время запуска или максимальное время работы, введите команду UPDATE SCHEDULE . Информацию об этой команде смотрите в разделе UPDATE SCHEDULE (Изменить запланированное задание клиента) .

Информация, связанная с данной

[QUERY ACTLOG \(Запросить информацию журнала операций\)](#)

Мониторинг оповещений ленточных устройств для выявления аппаратных ошибок

Оповещения ленточных устройств генерируются ленточными и библиотечными устройствами и сообщают об аппаратных ошибках. Эти сообщения помогают определить проблемы, не связанные с сервером.

Об этой задаче

Создается страница журнала, которую можно получить в любой момент времени или в определенный момент, например, при размонтировании накопителя.

У сообщения с оповещением ленточных устройств может быть один из следующих уровней серьезности:

- Информационное (например, при попытке загрузить картридж неподдерживаемого типа)
- Предупреждение (например, если ожидается аппаратная ошибка);
- Критическое (например, если возникли неполадки с лентой и данные в опасности).

По умолчанию оповещения ленточных устройств отключены.

Процедура

- Чтобы включить сообщения с оповещениями ленточных устройств, введите команду **SET TAPEALERTMSG** и задайте значение **ON**: `set tapealertmsg on`

- Чтобы проверить, включены ли сообщения с оповещениями ленточных устройств, введите команду **QUERY TAPEALERTMSG: query tapealertmsg**

Как избежать ошибок, связанных с несовместимостью носителей

Производя мониторинг и устраняя проблемы совместимости носителей, вы сможете предотвратить ошибки в решении на основе лент. Новый накопитель может иметь ограниченную возможность использования форматов носителей, поддерживаемых накопителем предыдущей версии. Часто новый дисковод может считывать, но не записывать носители в старом формате.

Об этой задаче

По умолчанию существующие тома, имеющие состояние FILLING, сохраняют это состояние после замены накопителя. В некоторых случаях для заполнения таких томов может возникнуть необходимость продолжать использование старого накопителя. При этом сохраняется возможность чтения и записи существующих томов до их освобождения. Если обновляются все накопители библиотеки, убедитесь, что форматы носителей поддерживаются новыми аппаратными средствами. Если с новыми накопителями планируется использовать не только новые носители, придется учитывать проблемы совместимости. Инструкции по переносу смотрите в разделе [“Перенос данных на обновленные накопители”](#) на стр. 217.

Чтобы использовать новый накопитель с носителями, которые он может считывать, но не записывать, введите команду **UPDATE VOLUME**, чтобы установить доступ к этим томам только для чтения. Это предотвратит ошибки, вызываемые несовместимостью чтения-записи. Например, новый накопитель может выбрасывать носители, записанные в формате, который он не поддерживает, сразу после загрузки в накопитель. Или же новый накопитель может не выполнить первую команду записи на носитель, частично записанный в неподдерживаемом формате.

Когда данные на носителе, предназначенном только для чтения, устареют и том будет освобожден, нужно будет заменить его носителем, полностью совместимым с новым накопителем. Ошибки могут возникать, если новому накопителю не удастся правильно откалибровать том, записанный в старом формате. Чтобы избежать этой проблемы, убедитесь, что исходный накопитель находится в исправном рабочем состоянии, а его микрокод - на текущем уровне.

Операции с чистящими картриджами

Чтобы убедиться, что ленточные накопители подвергаются очистке, когда это необходимо, и чтобы избежать проблем с пространством хранения на ленте, следуйте рекомендациям.

Мониторинг процесса очистки

Если в библиотеке активируется чистящий картридж и нужно очистить накопитель, сервер размонтирует том данных и запустит операцию очистки. Если операция очистки завершится неудачно или будет отменена либо если чистящего картриджа нет, вы можете не узнать, что требуется очистка накопителя. Из-за этой проблемы необходимо следить за сообщениями об очистке, чтобы обеспечить своевременную очистку накопителей. При необходимости введите команду **CLEAN DRIVE**, чтобы сервер попытался еще раз произвести очистку, или вручную загрузите чистящий картридж в накопитель.

Использование нескольких чистящих картриджей

Сервер будет использовать чистящий картридж для числа очисток, указанного при регистрации чистящего картриджа. Если зарегистрировать два или несколько чистящих картриджей, сервер будет использовать только один из них, пока не будет достигнуто заданное для картриджа число очисток. Затем сервер использует следующий чистящий картридж. Если зарегистрировать два или несколько чистящих картриджей и ввести две или несколько команд **CLEAN DRIVE** одновременно, сервер будет использовать несколько картриджей одновременно и зарегистрирует оставшееся количество очисток для каждого картриджа.

Информация, связанная с данной

[AUDIT LIBRARY \(аудит томов автоматизированной библиотеки\)](#)

[CHECKIN LIBVOLUME \(регистрация тома хранения в библиотеке\)](#)

CLEAN DRIVE (очистка накопителя)

LABEL LIBVOLUME (запись метки на том библиотеки)

QUERY LIBVOLUME (Запросить информацию о том библиотеки)

Проверка на соответствие лицензии

Убедитесь, что ваше решение IBM Spectrum Protect соответствует положениям вашего лицензионного соглашения. Регулярно производя мониторинг решения, можно отслеживать тенденции роста данных или использование единиц мощности процессора (processor value unit, PVU). Используйте эту информацию, чтобы спланировать будущее приобретение лицензий.

Об этой задаче

Метод, который вы используете, чтобы убедиться, что ваше решение соответствует условиям лицензии, зависит от положений вашего лицензионного соглашения IBM Spectrum Protect.

Фронтальное лицензирование мощности

Фронтальная модель определяет требования к лицензии на основе объема первичных данных, о которых клиентами было сообщено, что для них создавались резервные копии. К клиентам относятся приложения, виртуальные машины и компьютеры.

Внутреннее лицензирование мощности

Внутренняя модель определяет требования к лицензии на основе числа терабайт данных, которые хранятся в первичных пулах хранения и репозиториях.

Советы:

- Чтобы обеспечить точность оценки фронтальной и внутренней емкости, установите новейшую версию программы клиента на каждом клиентском узле.
- Информация о фронтальной и внутренней емкости в Центре операций предназначена только для планирования и оценки.

Лицензирование PVU

Модель PVU основана на использовании PVU серверными устройствами.



Важное замечание: Расчеты PVU, выполняемые IBM Spectrum Protect, считаются оценочными и не имеют юридической силы. Информация о лицензировании PVU, сообщенная продуктом IBM Spectrum Protect, не рассматривается как допустимая замена для IBM License Metric Tool. IBM License Metric Tool предназначен для отслеживания фактического использования. Например, после установки Клиент резервного копирования и архивирования IBM Spectrum Protect этот инструмент учитывает клиента только после первого использования. Дополнительную информацию о IBM License Metric Tool смотрите в разделе [IBM License Metric Tool](#).

Если у вас возникнут вопросы или замечания, касающиеся требований по лицензированию, обращайтесь к вашему поставщику программы IBM Spectrum Protect.

Процедура

Чтобы отследить соответствие лицензии, выполните шаги, соответствующие положениям вашего лицензионного соглашения.

Совет: Центр операций обеспечивает электронный отчет, в котором просуммировано использование фронтальной и внутренней емкости. Отчеты можно автоматически регулярно отправлять одному или нескольким получателям. Чтобы сконфигурировать электронные отчеты и управлять ими, щелкните по **Отчеты** в строке меню Центра операций.

Опция	Описание
Фронтальная модель	<p>a. В строке меню компонента Центр операций установите указатель мыши на значок параметров  и щелкните по Лицензирование.</p> <p>На странице Фронтальное использование показана оценка фронтальной емкости.</p> <p>b. Если в столбце Нет отчета показано значение, щелкните по числу, чтобы узнать о клиентах, которые не сообщили об использовании емкости.</p> <p>c. Чтобы оценить емкость для клиентов, которые не сообщают об использовании емкости, перейдите на следующий сайт скачивания, где предоставляются инструменты измерения и инструкции: https://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools</p> <p>Чтобы изменить фронтальную емкость в соответствии со сценарием, выполните инструкции в самом последнем доступном руководстве по лицензированию.</p> <p>d. Прибавьте оценку для компонента Центр операций и все оценки, которые вы получили с использованием сценария.</p> <p>e. Убедитесь, что оценка емкости соответствует вашему лицензионному соглашению.</p>
Внутренняя модель	<p>Ограничение: Если исходный и целевой серверы репликации не используют одни и те же параметры политики, вы не сможете использовать Центр операций для мониторинга использования внутренней емкости для реплицируемых клиентов. Информацию о том, как оценить использование емкости для этих клиентов, смотрите в следующей публикации technote 1656476.</p> <p>a. В строке меню компонента Центр операций установите указатель мыши на значок параметров  и щелкните по Лицензирование.</p> <p>b. Щелкните по вкладке Внутренний.</p> <p>c. Проверьте, соответствует ли оценка объема данных вашему лицензионному соглашению.</p>
Модель PVU	Информацию о том, как оценить соответствие условиям лицензирования PVU, смотрите в разделе Оценка соответствия модели лицензирования PVU .

Состояние системы отслеживания с использованием отчетов по электронной почте

Настройте компонент Центр операций, чтобы сгенерировать отчеты по электронной почте, в которых суммируется состояние системы. Вы можете сконфигурировать соединение с почтовым сервером, изменить параметры отчета и (необязательно) создать пользовательские отчеты.

Прежде чем начать

Прежде чем настраивать отчеты по электронной почте, убедитесь, что выполнены следующие требования:

- Доступен хост-сервер Simple Mail Transfer Protocol (SMTP) для отправки и получения отчетов по электронной почте. Сервер SMTP должен быть сконфигурирован как открытый почтовый ретранслятор. Вы также должны убедиться, что у сервера IBM Spectrum Protect, который отправляет сообщения электронной почты, есть доступ к серверу SMTP. Если центр операций установлен на отдельном компьютере, этому компьютеру не требуется доступ к серверу SMTP.
- Чтобы задавать отчеты по электронной почте, нужно иметь системные полномочия для сервера.
- Чтобы задать получателей, можно ввести один или несколько адресов электронной почты или ID администраторов. Если вы собираетесь ввести ID администратора, ID должен быть зарегистрирован на хаб-сервере и с ним должен быть связан адрес электронной почты. Чтобы задать адрес электронной почты для администратора, используйте параметр **EMAILADDRESS** в команде **UPDATE ADMIN**.

Об этой задаче

Вы можете сконфигурировать Центр операций для отправки отчета об общих операциях, отчета о соответствии лицензии, а также одного или нескольких пользовательских отчетов. Вы создаете пользовательские отчеты, выбирая шаблоны из набора обычно используемых шаблонов отчетов или вводя операторы SQL SELECT, чтобы запросить информацию на управляемых серверах.

Процедура

Чтобы настроить электронные отчеты и управлять ими, сделайте следующее:

1. В строке меню компонента Центр операций выберите **Отчеты**.
2. Если соединение с сервером электронной почты еще не сконфигурировано, щелкните по **Сконфигурировать почтовый сервер** и заполните поля.
После того как вы сконфигурируете почтовый сервер, будут включены отчет об общих операциях и отчет о соответствии лицензии.
3. Чтобы изменить параметры отчета, выберите отчет, щелкните по **Сведения** и обновите форму.
4. Необязательно: Чтобы добавить пользовательский отчет, щелкните по **+ Отчет** и заполните поля.

Совет: Чтобы сразу же запустить и отправить отчет, выберите отчет и нажмите на **Отправить**.

Результаты

Разрешенные отчеты будут отправлены в соответствии с заданными параметрами.

Дальнейшие действия

Отчет об общих операциях содержит вложение. Чтобы найти более подробную информацию, разверните разделы во вложении.

Если вам не удастся увидеть изображение в отчете, возможно, вы используете клиент электронной почты, который преобразует HTML в другой формат. Информацию об ограничениях смотрите в электронной справке по компоненту Центр операций.

Часть 4. Управление операциями для решения на лентах

Используйте эту информацию для управления операциями для реализации решения на лентах на сервере IBM Spectrum Protect.

Управление Центром операций

Центр операций предоставляет веб-доступ и мобильный доступ к информации о состоянии для среды IBM Spectrum Protect.

Об этой задаче

Используйте Центр операций для мониторинга нескольких серверов и для выполнения некоторых задач администрирования. Кроме того, Центр операций предоставляет веб-клиент для командной строки IBM Spectrum Protect. Дополнительную информацию об использовании Центра операций смотрите в разделе [Управление Центром операций](#).

Управление операциями клиентов

Вы можете устранить ошибки клиентов, управлять обновлением клиентов и списывать узлы клиентов, которые больше не нужны. Чтобы высвободить пространство хранения на сервере, можно деактивировать устаревшие данные, сохраненные клиентами приложений.

Об этой задаче

В некоторых случаях ошибки клиентов можно устранить, остановив и перезапустив приемник клиента. Если клиентские узлы или ID администратора окажутся заблокированы, вы сможете устранить проблему, разблокировав клиентский узел или ID администратора, а затем переустановив пароль.

Подробные инструкции по выявлению и устранению ошибок клиентов смотрите в разделе [Устранение проблем клиентов](#).

Инструкции по добавлению клиентов смотрите в разделе [“Защита приложений и компьютеров”](#) на стр. 112.

Оценка ошибок в журналах ошибок клиентов

Ошибки клиента можно устранить, получив рекомендации из компонента Центр операций или просмотрев журналы ошибок на клиенте.

Прежде чем начать

(Необязательно) Чтобы устранить ошибки на клиенте резервного копирования и архивирования в операционной системе Linux или Windows, убедитесь, что у вас установлен и запущен компонент служба управления клиентами. Инструкции по установке смотрите в разделе [Установка службы управления клиентом](#).

Процедура

Чтобы диагностировать и устранить ошибки клиента, выполните одно из следующих действий:

- Если служба службы управления клиентами установлена на клиентском узле, выполните следующие шаги:

- a) На странице обзора в компоненте Центр операций щелкните по **Клиенты** и выберите клиент.
- b) Щелкните по **Сведения**.
- c) На странице Сводка клиента щелкните по вкладке **Диагностика**.
- d) Прочтите полученные сообщения журнала.

Советы:

- Чтобы показать или скрыть панель Журналы клиента, дважды щелкните по строке Журналы клиента.
- Чтобы изменить размер панели Журналы клиента, щелкните по строке Журналы клиента и перетащите ее в нужное положение.

Если на странице Диагностика показаны рекомендации, выберите рекомендацию. В панели Журналы клиента сообщения журнала клиента, с которыми связаны рекомендации, выделены.

- e) Используйте рекомендации, чтобы устранить проблемы, указанные в сообщениях об ошибках.

Совет: Рекомендации предоставляются не для всех сообщений клиентов.

- Если служба управления клиентами не установлена на клиентском узле, смотрите журналы ошибок установленного клиента.

Остановка и перезапуск приемника клиента

Если вы измените конфигурацию вашего решения, вам нужно будет перезапустить приемник клиента на всех клиентских узлах, где установлен клиент резервного копирования и архивирования.

Об этой задаче

В некоторых случаях ошибки планирования клиентов можно устранить, остановив и перезапустив приемник клиента. Чтобы запланированные операции могли выполняться на клиенте, приемник клиента должен работать. Например, если вы измените IP-адрес или имя домена сервера, вы должны будете перезапустить приемник клиента.

Процедура

Следуйте инструкциям для операционной системы, установленной на клиентском узле:

AIX и Oracle Solaris

- Чтобы остановить приемник клиента, выполните следующие действия:
 - a. Определите ID процесса приемника клиента, введя в командной строке следующую команду:

```
ps -ef | grep dsmcad
```

Ознакомьтесь с выводом. В приведенном ниже примере выходной информации 6764 - это ID процесса приемника клиента:

```
root 6764      1   0 16:26:35 ?           0:00 /usr/bin/dsmcad
```

- b. Введите следующую команду в командной строке:

```
kill -9 PID
```

где *PID* задает ID процесса приемника клиента.

- Чтобы запустить приемник клиента, введите в командной строке следующую команду:

```
/usr/bin/dsmcad
```

Linux

- Чтобы остановить приемник клиента (но не перезапускать его), введите следующую команду:

```
# service dsmcad stop
```

- Чтобы остановить и перезапустить приемник клиента, введите следующие команды:

```
# service dsmcad restart
```

MAC OS X

Выберите **Приложения > Утилиты > Терминал**.

- Чтобы остановить приемник клиента, введите следующую команду:

```
/bin/launchctl unload -w com.ibm.tivoli.dsmcad
```

- Чтобы запустить приемник клиента, введите следующую команду:

```
/bin/launchctl load -w com.ibm.tivoli.dsmcad
```

Windows

- Чтобы остановить службу приемника клиента, выполните следующие действия:
 - a. Выберите **Пуск > Администрирование > Службы**.
 - b. Дважды щелкните по службе приемника клиента.
 - c. Щелкните по **Остановить** и **ОК**.
- Чтобы перезапустить службу приемника клиента, выполните следующие действия:
 - a. Выберите **Пуск > Администрирование > Службы**.
 - b. Дважды щелкните по службе приемника клиента.
 - c. Щелкните по **Запуск** и **ОК**.

Информация, связанная с данной

[Устранение проблем расписаний клиентов](#)

Изменение паролей

Если пароль для клиентского узла или ID администратора окажется потерян или забыт, вы можете переустановить пароль. Если будет предпринято несколько попыток получить доступ к системе с использованием неправильного пароля, это может привести к блокировке клиентского узла или ID администратора. Вы можете выполнить ряд шагов, чтобы устранить эту проблему.

Процедура

Чтобы устранить ошибки паролей, выполните одно из следующих действий:

- Если клиент резервного копирования и архивирования установлен на клиентском узле, а пароль был потерян или забыт, выполните следующие шаги:

1. Сгенерируйте новый пароль, введя команду **UPDATE NODE**:

```
update node имя_узла  
новый_пароль forcepwreset=yes
```

где *имя_узла* - это клиентский узел, а *новый_пароль* - это пароль, который вы назначаете.

2. Проинформируйте владельца клиентского узла об измененном пароле. Когда владелец клиентского узла входит в систему с использованием указанного пароля, новый пароль генерируется автоматически. Этот пароль неизвестен пользователям, чтоб позволяет сделать защиту более строгой.

Совет: Пароль генерируется автоматически, если вы ранее задали для опции **passwordaccess** значение **generate** в файле опций клиента.

- Если администратор окажется заблокирован из-за проблем, связанных с паролем, выполните следующие шаги:

1. Чтобы обеспечить администратору доступ к серверу, введите команду **UNLOCK ADMIN**. Инструкции смотрите в разделе [UNLOCK ADMIN \(разблокирование администратора\)](#).
2. Задайте новый пароль, используя команду **UPDATE ADMIN**:

```
update admin имя_администратора  
новый_пароль  
forcepwreset=yes
```

где *имя_администратора* - это имя администратора, а *новый_пароль* - это пароль, который вы назначаете.

- Если клиентский узел заблокирован, выполните следующие шаги:
 1. Определите, почему клиентский узел заблокирован и нужно ли его разблокировать. Например, если клиентский узел окажется списан, он удаляется из производственной среды. Обратить операцию списания нельзя, и клиентский узел останется заблокированным. Клиентский узел также может оказаться заблокированным, если данные клиента являются предметом юридического изучения.
 2. Если вам нужно разблокировать клиентский узел, используйте команду **UNLOCK NODE**. Инструкции смотрите в разделе [UNLOCK NODE \(Разблокировать клиентский узел\)](#).
 3. Сгенерируйте новый пароль, введя команду **UPDATE NODE**:

```
update node имя_узла  
новый_пароль forcepwreset=yes
```

где *имя_узла* задает имя узла, а *новый_пароль* - это пароль, который вы назначаете.

4. Проинформируйте владельца клиентского узла об измененном пароле. Когда владелец клиентского узла входит в систему с использованием указанного пароля, новый пароль генерируется автоматически. Этот пароль неизвестен пользователям, чтоб позволяет сделать защиту более строгой.

Совет: Пароль генерируется автоматически, если вы ранее задали для опции **passwordaccess** значение **generate** в файле опций клиента.

Управление обновлениями клиентов

Когда появится пакет исправлений или промежуточное исправление для клиента, вы сможете обновить клиент, чтобы воспользоваться преимуществами в улучшенном продукте. Серверы и клиенты можно обновлять в разное время, и они могут находиться на разных уровнях (с некоторыми ограничениями).

Прежде чем начать

1. Прочтите требования к совместимости клиентов/серверов в разделе [Замечания о совместимости и обновлении IBM Spectrum Protect](#) . Если ваше решение включает в себя серверы или клиенты с более ранним уровнем версии, чем V7.1, смотрите рекомендации, чтобы убедиться, что операции резервного копирования и архивирования клиента не будут нарушены.
2. Узнайте о требованиях к системе для клиента в разделе [Поддерживаемые операционные системы для IBM Spectrum Protect](#).
3. Если решение содержит агенты хранения или библиотечные клиенты, ознакомьтесь с информацией о совместимости агентов хранения и библиотечных клиентов с серверами, сконфигурированными в качестве менеджеров библиотек. Смотрите раздел [Совместимость агента хранения и библиотечного клиента с сервером IBM Spectrum Protect](#) .

Если вы собираетесь обновить менеджера библиотек и библиотечный клиент, сначала нужно обновить менеджера библиотек.

Процедура

Для обновления программного обеспечения выполните инструкции, перечисленные в следующей таблице.

Программа	Ссылка на инструкции
Клиент резервного копирования и архивирования IBM Spectrum Protect	<ul style="list-style-type: none">• Планирование обновлений клиентов
IBM Spectrum Protect Snapshot	<ul style="list-style-type: none">• Установка и обновление IBM Spectrum Protect Snapshot for UNIX and Linux• Установка и обновление IBM Spectrum Protect Snapshot for VMware• Установка и обновление IBM Spectrum Protect Snapshot for Windows
IBM Spectrum Protect for Databases	<ul style="list-style-type: none">• Обновление Data Protection for SQL Server• Установка Data Protection for Oracle• Установка, обновление и перенастройка IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Enterprise Resource Planning	<ul style="list-style-type: none">• Обновление IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Db2• Обновление IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle
IBM Spectrum Protect for Mail	<ul style="list-style-type: none">• Установка Data Protection for IBM Domino в системе UNIX, AIX или Linux (V7.1.0)• Установка Data Protection for IBM Domino в системе Windows (V7.1.0)• Установка, обновление и перенастройка IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Virtual Environments	<ul style="list-style-type: none">• Установка и обновление Data Protection for VMware• Установка и обновление Data Protection for Microsoft Hyper-V

Списание клиентского узла

Если клиентский узел больше не требуется, можно запустить процесс для его удаления из производственной среды. Например, если рабочая станция производила резервное копирование данных на сервер IBM Spectrum Protect, но рабочая станция больше не используется, рабочую станцию можно списать (вывести из использования).

Об этой задаче

При запуске процесса списания сервер блокирует клиентский узел, чтобы помешать ему получить доступ к серверу. Файлы, принадлежащие клиентскому узлу, постепенно удаляются, и затем удаляется клиентский узел. Можно списать следующие типы клиентских узлов:

Клиентские узлы приложения

К клиентским узлам приложений относятся серверы электронной почты, базы данных и другие приложения. Например, клиентским узлом приложения может быть любое из следующих приложений:

- IBM Spectrum Protect Snapshot

- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

Клиентские узлы компьютеров

В число клиентских узлов компьютеров входят рабочие станции, серверы файлов NAS и клиенты API.

Клиентские узлы виртуальных машин

Клиентские узлы виртуальных машин представляют собой отдельные хосты-гости в гипервизоре. Каждая виртуальная машина представлена как файловое пространство.

Ограничение: Нельзя списать клиентский узел объектов.

Простейший метод списания клиентского узла заключается в том, чтобы использовать Центр операций. Процесс списания выполняется в фоновом режиме. Если клиент сконфигурирован для репликации данных клиента, Центр операций, прежде чем списать клиент, автоматически удалит клиент из репликации на исходном и целевом серверах репликации.

Совет: Либо можно списать клиентский узел, введя команду **DECOMMISSION NODE** или **DECOMMISSION VM**. Вы можете счесть целесообразным использовать этот метод в следующих случаях:

- Чтобы запланировать процесс списания на будущее или выполнить ряд команд, используя сценарий, задайте выполнение процесса списания в фоновом режиме.
- Чтобы производить мониторинг процесса списания с целью отладки, задайте выполнение процесса списания в фоновом режиме. Если вы запустите процесс в активном режиме, вам придется дождаться завершения процесса, прежде чем вы сможете перейти к другим задачам.

Процедура

Выполните одно из следующих действий.

- Чтобы списать клиент в фоновом режиме, используя Центр операций, выполните следующие действия:
 - а) На странице **Обзор** для компонента Центр операций щелкните по **Клиенты** и выберите клиент.
 - б) Выберите **Еще > Списать**.
- Чтобы списать клиентский узел, используя команду администрирования, выполните одно из следующих действий:
 - Чтобы списать клиентские узлы приложений или системные клиентские узлы в фоновом режиме, введите команду **DECOMMISSION NODE**. Например, если имя клиентского узла - AUSTIN, введите следующую команду:

```
decommission node austin
```

- Чтобы списать клиентские узлы приложений или системные клиентские узлы в активном режиме, введите команду **DECOMMISSION NODE** и задайте параметр wait=yes. Например, если имя клиентского узла - AUSTIN, введите следующую команду:

```
decommission node austin wait=yes
```

- Чтобы списать виртуальную машину в фоновом режиме, введите команду **DECOMMISSION VM**. Например, если имя виртуальной машины - AUSTIN, файловое пространство - 7, а имя файлового пространства задано с помощью ID файлового пространства, введите следующую команду:

```
decommission vm austin 7 nametype=fsid
```

Если имя виртуальной машины содержит один или несколько пробелов, заключите имя в двойные кавычки. Например:

```
decommission vm "austin 2" 7 nametype=fsid
```

- Чтобы списать виртуальную машину в активном режиме, введите команду **DECOMMISSION VM** и задайте параметр `wait=yes`. Например, введите следующую команду:

```
decommission vm austin 7 nametype=fsid wait=yes
```

Если имя виртуальной машины содержит один или несколько пробелов, заключите имя в двойные кавычки. Например:

```
decommission vm "austin 2" 7 nametype=fsid wait=yes
```

Дальнейшие действия

Следите за сообщениями об ошибках, которые могут появиться в пользовательском интерфейсе или в выходной информации команды сразу после запуска процесса.

Можно проверить, списан ли клиентский узел:

1. Щелкните на странице **Обзор** в компоненте Центр операций по **Клиенты**.
2. В таблице Клиенты проверьте состояние в столбце Под угрозой:
 - Состояние **DECOMMISSIONED** (Списан) указывает, что узел списан.
 - Нулевое значение указывает, что узел не списан.
 - Состояние **PENDING** (Отложено) указывает, что узел списывается или процесс списания завершился неудачно.

Совет: Если вы хотите определить состояние отложенного процесса списания, введите следующую команду:

```
query process
```

3. Ознакомьтесь с выводом команды:

- Если указано состояние для процесса списания, процесс выполняется. Например:

```
query process

  Номер    Описание процесса    Состояние процесса
  Число
-----
      3      DECOMMISSION NODE      Number of backup objects deactivated
                                   for node NODE1: 8 objects deactivated.
```

- Если для процесса списания никакого состояния не указано и вы не получили сообщения об ошибке, процесс не завершен. Процесс может быть не завершен, если файлы, связанные с узлом, еще не деактивированы. После деактивации файлов снова запустите процесс списания.
- Если для процесса списания никакого состояния не указано и вы получили сообщения об ошибке, это означает, что процесс завершился неудачно. Еще раз запустите процесс списания.

Совет: Чтобы сбросить состояние узла или виртуальной машины, которые были ранее списаны, используйте следующие административные команды:

- Чтобы сбросить состояние узла, который был ранее списан из производственной среды при помощи команды **DECOMMISSION NODE**, используйте команду **RECOMMISSION NODE**.
- Чтобы сбросить состояние файлового пространства виртуальной машины, которое было ранее списано из производственной среды при помощи команды **DECOMMISSION VM**, используйте команду **RECOMMISSION VM**.

Информация, связанная с данной

[DECOMMISSION NODE \(Списать клиентский узел\)](#)

[DECOMMISSION VM \(Списать виртуальную машину\)](#)

Деактивация данных для высвобождения пространства хранения

В некоторых случаях можно деактивировать данные, хранящиеся на сервере IBM Spectrum Protect. Когда вы запустите процесс деактивации, все резервные копии данных, сохраненные до указанной даты и времени, деактивируются и будут удалены, когда истечет срок их действия. Таким способом можно высвобождать пространство на сервере.

Об этой задаче

Некоторые клиенты приложений всегда сохраняют данные на сервере как активные резервные копии данных. Поскольку активные резервные копии данных не управляются политиками устаревания перечня, данные не удаляются автоматически, и серверная система хранения используется до бесконечности. Чтобы высвободить пространство хранения, используемое устаревшими данными, можно деактивировать данные.

Когда вы запускаете процесс деактивации, все активные резервные копии данных, сохраненные до указанной даты, станут неактивными. Данные будут удалены по мере истечения срока их хранения, и восстановить их будет нельзя. Функция деактивации применяется только к клиентам приложений, которые защищают базы данных Oracle.

Процедура

1. На странице обзора в компоненте Центр операций щелкните по **Клиенты**.
2. В таблице Клиенты выберите один или несколько клиентов и щелкните по **Еще > Очистить**.

Метод командной строки: Деактивируйте данные, используя команду **DEACTIVATE DATA**.

Информация, связанная с данной

[DEACTIVATE DATA \(деактивация данных для клиентского узла\)](#)

Управление системой хранения данных

Управляйте данными эффективно и добавляйте на сервер поддерживаемые устройства и носители, чтобы хранить данные клиента.

Related information

[Типы пулов хранения](#)

Управление емкостью перечня

Управляйте емкостью базы данных, активного журнала и архивных журналов, чтобы размер перечня определялся для задач на основе состоянии журналов.

Прежде чем начать

У активного и архивного журналов есть следующие особенности:

- Максимальный размер активного журнала равен 512 ГБ. Более подробную информацию о размерах активного журнала для вашей системы смотрите в разделе [“Планирование массивов хранения”](#) на стр. 15.
- Размер архивного журнала ограничен размером файловой системы, в которой он установлен. Размер архивного журнала не поддерживается на заранее заданном уровне, как в случае активного журнала. Архивные файлы журналов автоматически удаляются, когда они становятся больше не нужны.

(Необязательно) Лучше всего создать архивный журнал отказоустойчивости, чтобы сохранять файлы архивного журнала при переполнении каталога архивных журналов.

Проверьте Центр операций, чтобы определить, какой компонент перечня переполняется. Прежде чем увеличивать размер одного из компонентов перечня, убедитесь, чтобы вы остановили сервер.

Процедура

- Чтобы увеличить размер дискового пространства для базы данных, выполните следующие шаги:
 - Создайте один или несколько каталогов для базы данных на отдельных накопителях или в файловых системах.
 - Введите команду **EXTEND DBSPACE**, чтобы добавить каталог или каталоги к базе данных. Каталоги должны быть доступны для ID пользователя экземпляра менеджера базы данных. По умолчанию данные перераспределяются по всем каталогам базы данных и пространство освобождается.

Советы:

- Время, необходимое для полного перераспределения данных и освобождения пространства, изменяется в зависимости от размера вашей базы данных. Убедитесь, что это учтено при планировании.
- Убедитесь, что размер указанных каталогов совпадает с размером существующих каталогов, чтобы обеспечить согласованную степень параллелизма для операций базы данных. Если один или более каталогов для базы данных окажутся меньше других, это уменьшит оптимизированное параллельное упреждающее чтение и распределение базы данных.
- Остановите и перезапустите сервер для полного использования новых каталогов.
- Если потребуется, исправьте базу данных. Реорганизация индекса и таблиц для базы данных сервера может помочь избежать неожиданных проблем, связанных с ростом базы данных и производительностью. Дополнительную информацию о реорганизации базы данных смотрите в [Разрешение и предотвращение проблем, связанных с ростом базы данных и сниженной производительностью в Tivoli Storage Manager V7.1.1.200 и более поздних серверах](#).
- Чтобы узнать, как уменьшить размер базы данных для серверов V7.1 и новее, смотрите информацию в разделе [Разрешение и предотвращение проблем, связанных с ростом базы данных и сниженной производительностью в Tivoli Storage Manager V7.1.1.200 и более поздних серверах](#).

Ограничение: Команды могут увеличить число операций ввода-вывода и повлиять на производительность сервера. Чтобы свести к минимуму проблемы производительности, подождите выполнения одной команды перед вводом следующей команды. Команды Db2 можно вводить, когда сервер работает.

- Чтобы увеличить или уменьшить размер активного журнала, выполните следующие шаги:
 - a) Убедитесь, что в каталоге активного журнала достаточно пространства для увеличения размера журнала.
 - b) Отключите сервер.
 - c) Измените в файле `dsmserv.opt` значение опции **ACTIVELOGSIZE**, задав новый размер активного журнала (в мегабайтах).

Размер файла активного журнала основан на значении опции ACTIVELOGSIZE.

Рекомендации по требованиям к объему пространства приведены в следующей таблице:

Таблица 29. Как оценить требования к пространству томов и файлов

Значение опции ACTIVELOGSize	Зарезервируйте этот объем свободного пространства в каталоге активного журнала в дополнение к пространству ACTIVELOGSize .
16 ГБ - 128 ГБ	5120 МБ
129 ГБ - 256 ГБ	10240 МБ
257 ГБ - 512 ГБ	20480 МБ

Чтобы изменить размер активного журнала до максимального размера, равного 512 ГБ, введите следующую серверную опцию:

```
activelogsize 524288
```

- d) Если вы собираетесь использовать новый каталог активного журнала, измените имя каталога, заданное серверной опцией **ACTIVELOGDIRECTORY**. Новый каталог должен быть пустым, и он должен быть доступен для ID пользователя менеджера базы данных.
- e) Перезапустите сервер.
- Произведите сжатие архивных журналов, чтобы уменьшить объем пространства, необходимого для хранения.
Разрешите динамическое сжатие архивного журнала следующей командой:

```
setopt archlogcompress yes
```

Ограничение: Будьте внимательны, если вы разрешаете опцию сервера **ARCHLOGCOMPRESS** на компьютерах с постоянным высоким использованием томов и высокими рабочими нагрузками. Разрешение этой опции в такой среде может привести к задержкам при архивировании файлов журнала из файловой системы активного журнала в файловую систему архивного журнала. Задержка может привести к тому, что в файловой системе активного журнала не хватит места. Обязательно выполняйте мониторинг пространства, доступного в файловой системе активного журнала, после разрешения сжатия архивного журнала. Если использование файловой системы каталога активного журнала приближается к предельному, то запретите опцию сервера **ARCHLOGCOMPRESS**. Чтобы немедленно запретить сжатие архивного журнала без остановки сервера, введите команду **SETOPT**.

Информация, связанная с данной

[ACTIVELOGSIZE](#), серверная опция

[EXTEND DBSPACE](#) (увеличение емкости базы данных)

[SETOPT](#) (Задать динамическое обновление серверной опции)

Тонкая настройка запланированных операций

Запланируйте ежедневное выполнение задач по обслуживанию, чтобы убедиться, что ваше решение работает правильно. Производя тонкую настройку решения, вы получаете максимальную отдачу от ресурсов сервера и эффективно используете другие функции, которые есть в вашем решении.

Процедура

1. Регулярно отслеживайте производительность системы, чтобы убедиться, что задачи по резервному копированию и обслуживанию выполняются успешно. Дополнительную информацию о мониторинге смотрите в разделе [Часть 3, “Мониторинг решения на лентах”](#), на стр. 143.

2. Если информация мониторинга показывает, что рабочая нагрузка сервера повышается, вам, возможно, следует проверить информацию планирования. Проверьте, является ли емкость системы достаточной, в следующих случаях:
 - Число клиентов увеличивается
 - Объем данных, резервное копирование которых производится, возрастает
 - Время, доступное для резервного копирования, изменяется
3. Определите, есть ли в вашем решении проблемы, отрицательно влияющие на производительность.
Проверьте расписания клиентов, чтобы выяснить, выполняются ли задачи в течение запланированного периода времени:
 - a. Выберите клиента на странице **Клиенты** Центра операций.
 - b. Щелкните по **Сведения**.
 - c. На странице **Сводка** на клиенте проверьте операции **Создана резервная копия** и **Реплицирован**, чтобы выявить все риски.Скорректируйте время и частоту операций резервного копирования клиента, если потребуется.
4. Запланируйте достаточно времени для следующих задач по обслуживанию, чтобы они успешно выполнялись в течение 24-часового периода:
 - a. Создание резервной копии базы данных
 - b. Запускайте обработку устаревания, чтобы удалить резервные и архивные копии файлов из серверной системы хранения.

Информация, связанная с данной

Дедупликация данных (V7.1.1)

Производительность

Оптимизация операций путем включения совместного размещения файлов клиентов

Совместное размещение файлов клиентов сокращает число монтирований томов, которые требуются, когда пользователи восстанавливают, получают или возвращают много файлов из пула хранения. В результате сокращается общее время выполнения этих операций.

Об этой задаче

При включенном совместном размещении сервер пытается разместить все файлы в минимальном количестве томов хранения с последовательным доступом. Эти файлы могут принадлежать к одному клиентскому узлу, к группе клиентских узлов, к файловому пространству или к группе файловых пространств. Совместное размещение можно задать для каждого пула устройств с последовательным доступом при создании определения этого пула или при обновлении его характеристик.

Рисунок 7 на стр. 178 демонстрирует пример совместного размещения данных на уровне клиентского узла для трех клиентов — данные каждого из них содержатся на отдельном томе.

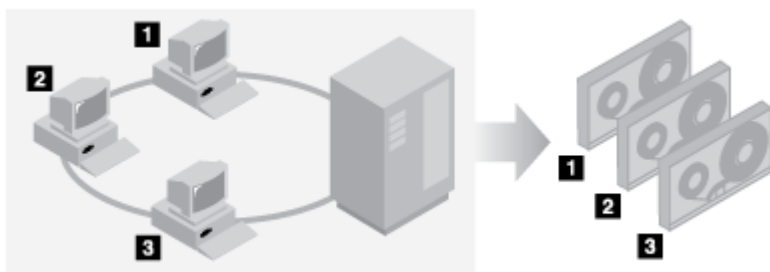


Рисунок 7. Пример совместного размещения, разрешаемого на узле

Рисунок 8 на стр. 178 демонстрирует пример совместного размещения данных на уровне группы клиентских узлов. Всего определены три группы, и данные каждой из них хранятся на отдельном наборе томов.

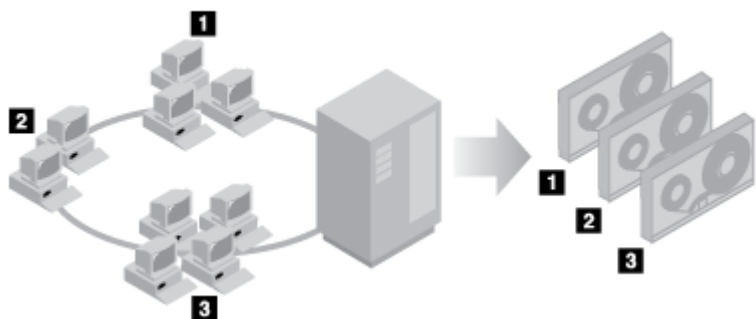


Рисунок 8. Пример совместного размещения, разрешаемого в группе совместного размещения на узле

Рисунок 9 на стр. 178 демонстрирует пример совместного размещения данных на уровне групп из файловых пространств. Определено шесть групп. Каждая группа содержит данные из файловых пространств, принадлежащих одному узлу. Данные для каждой группы хранятся в отдельном томе.

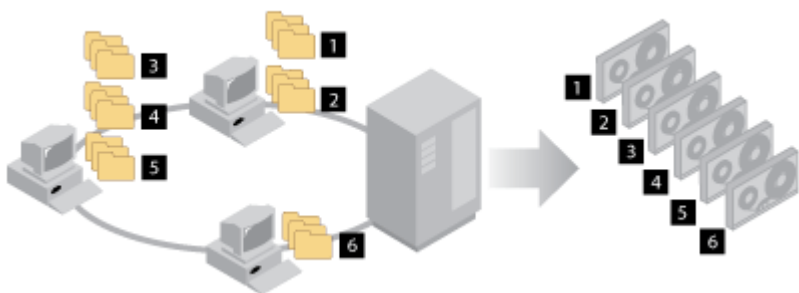


Рисунок 9. Пример совместного размещения, разрешенного в группе совместного размещения файлового пространства

Когда функция совместного размещения отключена, сервер пытается использовать все доступное пространство очередного тома назначения, и только потом начинает запись на следующий том. Хотя такой способ работы позволяет обходиться меньшим числом томов, пользовательские файлы оказываются разбросанными по многим томам. Рисунок 10 на стр. 179 демонстрирует пример конфигурации с отключенной функцией совместного размещения, когда пространство одного тома совместно используется тремя клиентами.

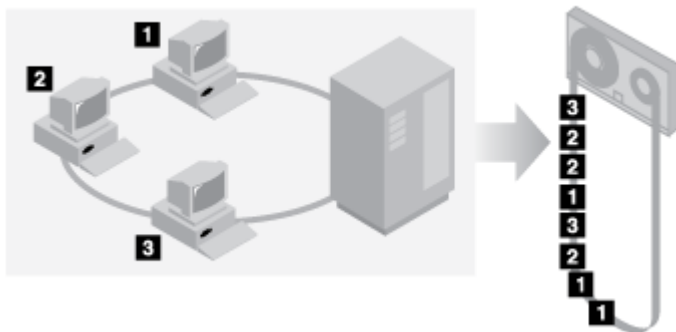


Рисунок 10. Пример конфигурации с отключенной функцией совместного размещения

Когда функция совместного размещения отключена, при выполнении пользовательских операций восстановления, извлечения из архива или возврата большого количества файлов производится большее число операций монтирования томов.

По умолчанию для первичных пулов томов с последовательным доступом сервер IBM Spectrum Protect осуществляет совместное размещение на уровне группы. Значение по умолчанию для пулов хранения копий и пулов длительного хранения - без совместного размещения.

Влияние функции совместного размещения на выполнение операций

Влияние функции совместного размещения на ресурсы и производительность системы зависит от типа выполняемых операций.

Таблица 30 на стр. 179 содержит сводную информацию о воздействии функции совместного размещения на выполнение различных операций.

Таблица 30. Влияние функции совместного размещения на выполнение операций

Операция	Функция совместного размещения включена	Функция совместного размещения отключена
Резервное копирование, архивация или перенос клиентских файлов	Для совместного размещения файлов производится больше операций монтирования	Требуется меньше операций монтирования носителей.
Восстановление, извлечение или возврат клиентских файлов	Восстановление, извлечение из архива или возврат большого количества клиентских файлов производится быстрее, поскольку файлы размещены на меньшем числе томов	Для каждого пользователя может производиться несколько операций монтирования, поскольку файлы бывают разбросаны по разным томам. На одном томе с последовательным доступом могут находиться файлы нескольких пользователей. Например, если два пользователя пытаются восстановить файлы в одном томе, один из пользователей будет вынужден дожидаться, когда будут восстановлены файлы другого пользователя.

Таблица 30. Влияние функции совместного размещения на выполнение операций (продолжение)

Операция	Функция совместного размещения включена	Функция совместного размещения отключена
Сохранение данных на ленте	Сервер задействует большое число ленточных томов, пытаясь сохранять файлы разных пользователей на разных томах, и лишь когда доступного пространства не остается, он может записать файлы разных пользователей на один том.	Сервер пытается использовать все доступное пространство очередной ленты, и лишь когда оно исчерпывается, сервер начинает использовать другую ленту.
Монтирование носителей	При резервном копировании, архивировании или переносе клиентских файлов прямо на тома с последовательным доступом требуется большее число операций монтирования. Также больше операций монтирования требуется при освобождении и при переносе данных из пула хранения. Управляется большее число томов, поскольку они заполняются не до конца.	При восстановлении, извлечении из архива и возврате клиентских файлов требуется больше операций монтирования.
Генерирование резервных наборов	Тратится меньше времени на поиск записей в базах данных и требуется выполнение меньшего количества операций монтирования.	Тратится больше времени на поиск записей в базах данных и требуется выполнение меньшего количества операций монтирования.
Копирование данных наборов хранения на ленту Важное замечание: Ваши параметры совместного размещения могут значительно увеличить число ленточных томов, требующихся набору хранения.	Сервер пытается сохранить файлы с одного совместно размещенного объекта на возможно меньшем числе ленточных томов. Время обработки для записи набора хранения на ленту может увеличиться.	Сервер пытается использовать все доступное пространство очередной ленты, и лишь когда оно исчерпывается, сервер начинает использовать другую ленту. Если нужно восстановить данные из набора хранения, для одного пользователя набора хранения может потребоваться больше операций монтирования ленты, так как файлы могут быть распределены по нескольким томам.

Если для группы, одного узла клиента или файлового пространства включено совместное размещение, все данные, принадлежащие этой группе, узлу или файловому пространству, перемещаются или копируются в ходе одного серверного процесса. Например, если данные совместно размещаются по группам, все данные для всех узлов, принадлежащих одной группе совместного размещения, переносятся одним процессом.

При совместном размещении данных сервер IBM Spectrum Protect пытается разместить все файлы на минимальном числе томов с последовательным доступом. Однако, когда сервер выполняет резервное копирование данных на тома с последовательным доступом, установки резервного

копирования имеют приоритет перед установками совместного размещения. В результате этого сервер выполняет операцию резервного копирования, но не может совместное разместить данные.

Предположим, например, что совместное размещение осуществляется на уровне узла и этому узлу разрешено использовать две точки монтирования на сервере. Предположим также, что при резервном копировании данные с этого узла легко помещаются на один ленточный том. Выполняя резервное копирование, сервер может смонтировать два тома, и в результате данные узла могут оказаться распределенными между двумя лентами. Если включить совместное размещение, следующие операции сервера будут использовать один серверный процесс:

- Перемещение данных с томов с произвольным или последовательным доступом.
- Перемещение данных узла с томов с последовательным доступом.
- Резервное копирование пула хранения с произвольным или последовательным доступом.
- Восстановление пула хранения с последовательным доступом.
- Освобождение пространства в пуле хранения с последовательным доступом или на томах вне площадки
- Перенос данных из пула хранения с произвольным доступом

При переносе данных из дискового пула хранения с произвольным доступом в пул хранения с последовательным доступом, когда совместное размещение производится на основе узлов или файловых пространств, узлы или файловые пространства автоматически выбираются для переноса на основе объема данных, подлежащего переносу. Для узла или файлового пространства с максимальным количеством таких данных перенос осуществляется в первую очередь. Если же совместное размещение осуществляется на уровне групп узлов, все узлы, связанные с пулом хранения, оцениваются на предмет наличия максимального количества подлежащих переносу данных. Сначала переносятся данные с узла с наибольшим количеством данных вместе со всеми данными для узлов, принадлежащих данной группе совместного размещения. Этот процесс выполняется независимо от того, сколько данных хранится в файловых пространствах узлов, и от того, был ли достигнут нижний порог переноса.

Однако когда вы переносите совместно размещенные данные из пула хранения с последовательным доступом в другой пул хранения с последовательным доступом, сервер заказывает тома в соответствии с датой, когда в последний раз осуществлялся доступ к тому. Первым переносится том с самой ранней датой обращения к нему, а последним - том с самой поздней датой доступа.

Одной из причин, почему совместное размещение лучше осуществлять по группам, является то, что отдельные клиентские узлы часто не имеют достаточного количества данных для заполнения ленточного тома высокой емкости. Поэтому совместное размещение на уровне групп позволяет уменьшить объем неиспользуемого пространства на лентах. Кроме того, совместное размещение данных по группам файловых пространств значительно сокращает объем неиспользуемых лент.

Данные, принадлежащие ко всем узлам в одной группе совместного размещения, переносятся в одном процессе. Поэтому совместное размещение по группам может сократить число раз, когда нужно монтировать том, подлежащий переносу. А еще при этом ускоряется сканирование базы данных и сокращается число проходов по лентам во время переноса данных из одного пула хранения с последовательным доступом в другой.

Выбор томов с включенным совместным размещением

Выбор томов зависит от того, производится ли совместное размещение по группам, узлам или файловым пространствам.

Таблица 31 на стр. 182 содержит критерии выбора сервером IBM Spectrum Protect первого тома, когда для пула хранения включена функция совместного размещения на уровне клиентских узлов, их групп или файловых пространств. Эти критерии применяются по очереди в указанном в таблице порядке, то есть в случае, когда отсутствует том, удовлетворяющий критерию 1, сервер ищет том, удовлетворяющий критерию 2 и т. д.

Таблица 31. Как сервер выбирает тома при включенной функции совместного размещения

Критерий выбора тома	Совместное размещение на уровне групп	Совместное размещение на уровне узлов	Совместное размещение на уровне файловых пространств
1	Том, уже содержащий файлы узлов из группы совместного размещения, к которой принадлежит клиент	Том, который уже содержит файлы того же клиентского узла	Том, который уже содержит файлы того же файлового пространства того же клиентского узла
2	Пустой заранее определенный том	Пустой заранее определенный том	Пустой заранее определенный том
3	Пустой чистый том	Пустой чистый том	Пустой чистый том
4	Том с наибольшим объемом свободного пространства из числа томов, уже содержащих данные	Том с наибольшим объемом свободного пространства из числа томов, уже содержащих данные	Том, содержащий данные с одного клиентского узла
5	Неприменимо	Неприменимо	Том с наибольшим объемом свободного пространства из числа томов, уже содержащих данные

Когда сервер должен продолжить сохранение данных уже во втором томе, он использует следующий порядок выбора для доступности большего пространства:

1. Пустой заранее определенный том
2. Пустой чистый том
3. Том с наибольшим объемом свободного пространства из числа томов, уже содержащих данные
4. Любой доступный том пула хранения

Когда совместное размещение организовано на уровне клиентского узла или файлового пространства, сервер пытается обеспечить наилучшее использование индивидуальных томов и минимизировать в томах перемешивание файлов от различных клиентов или из разных файловых пространств. Эта конфигурация показана на [Рисунок 11 на стр. 183](#), где видно, что выбор томов осуществляется *по горизонтали*, то есть перед тем, как будет использовано все доступное пространство каждого тома, осуществляется запись на все доступные тома. А, В, С и D - это файлы с четырех разных клиентских узлов.

Советы:

1. Если совместное размещение осуществляется на уровне клиентских узлов и узел содержит несколько файловых пространств, сервер не пытается совместно размещать файлы каждого из файловых пространств.
2. Если совместное размещение осуществляется на уровне файловых пространств и узел содержит их несколько, сервер пытается размещать файлы разных файловых пространств на разных томах.

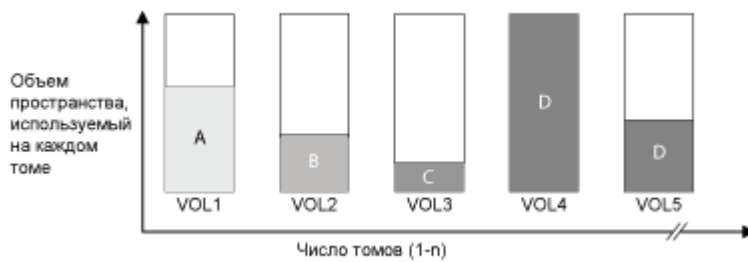


Рисунок 11. Использование всех доступных томов хранения с последовательным доступом с включенным совместным размещением на уровне узлов или файловых пространств

Совместное размещение может производиться на основе группы файловых пространств или группы узлов. Когда совместное размещение выполняется по группе узлов (группа совместного размещения по узлам), сервер пытается совместно разместить данные из узлов, принадлежащих к одной группе совместного размещения. Группа совместного размещения на основе файловых пространств использует те же методы, что и группа совместного размещения на основе узлов, но может использовать больше пространства, благодаря детализации размеров файловых пространств. В Рисунок 12 на стр. 183 показан пример, как размещаются данные для следующих групп узлов:

- группы 1, состоящей из узлов A, B и C;
- группы 2, состоящей из узлов D и E;
- группы 3, состоящей из узлов F, G, H и I

При возможности сервер IBM Spectrum Protect совместно размещает данные, принадлежащие группе узлов на одной ленте, представленной на рисунке Группой 2. Данные одного узла можно распределить также по нескольким лентам, связанным с группой (Группа 1 и Группа 2). Если узлы из одной группы размещения содержат по несколько файловых пространств, сервер не пытается размещать совместно данные каждого конкретного файлового пространства.

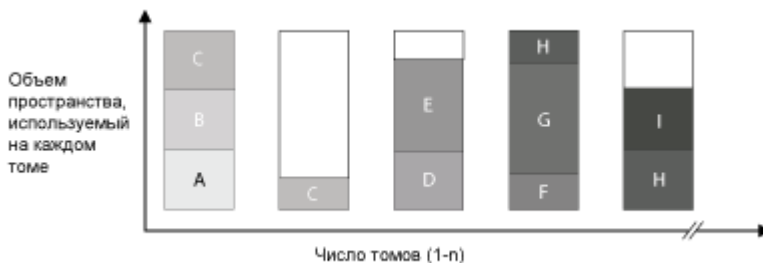


Рисунок 12. Использование всех доступных томов хранения с последовательным доступом с включенным совместным размещением на уровне групп

Обычно для выполняемой операции сервер IBM Spectrum Protect всегда записывает данные в текущий заполняемый том. Однако иногда можно заметить в совместно размещенном пуле хранения более одного заполняемого тома. В пуле совместного хранения может оказаться несколько заполняемых томов, если различные процессы сервера или сеансы клиента пытаются одновременно сохранить данные в пуле совместного размещения. В этой ситуации IBM Spectrum Protect выделит том для каждого процесса или сеанса, которому требуется том, так чтобы обе операции выполнялись как можно быстрее.

Выбор томов с выключенным совместным размещением

Когда функция совместного размещения отключена, сервер сначала пытается использовать все свободное пространство одного тома и лишь потом обращается к следующему тому.

При хранении файлов клиента в пуле хранения с последовательным доступом, для которого выключено совместное размещение, сервер выбирает том, используя следующий порядок выбора:

1. Использувавшийся ранее том с последовательным доступом, на котором имеется свободное пространство (при этом первым выбирается том с наибольшим количеством данных)
2. Пустой том

Когда свободное пространство текущего тома исчерпывается и серверу требуется продолжить сохранение данных на другом томе, он ищет в пуле свободный том. Если никаких пустых томов не существует, сервер попытается выбрать любой из оставшихся доступных томов в пуле хранения.

На [Рисунок 13 на стр. 184](#) показано, что при выключенном совместном размещении использование томов осуществляется по вертикали. В этом примере используется меньшее число томов, поскольку сервер пытается заполнить все доступное пространство каждого тома, записывая туда файлы разных клиентов. Столбцы A, B, C и D представляют данные с четырех разных клиентских узлов.

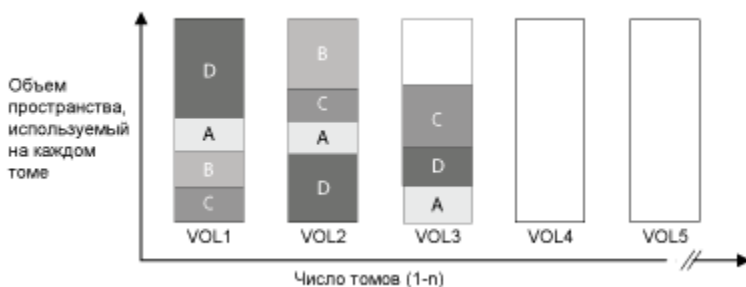


Рисунок 13. Использование всего доступного пространства на томах с последовательным доступом с выключенным совместным размещением

Параметры совместного размещения

Существует возможность изменить параметр совместного размещения для уже заданного пула хранения, обновив характеристики этого пула хранения. Это изменение не повлияет на размещение файлов, уже находящихся в пуле.

Например, если совместное размещение выключено для пула хранения, а вы его включите, с этого момента файлы клиента, хранящиеся в пуле, будут размещаться совместно. Файлы, которые ранее хранились в пуле хранения, не перемещаются для их совместного размещения. По мере освобождения или восстановления томов данные в пуле становятся все менее и менее совместно размещенными. Также можно использовать команды **MOVE DATA** или **MOVE NODEDATA** для перемещения данных на новые тома, чтобы повысить степень совместного размещения. Перемещение данных на новые тома вызывает увеличение времени обработки и объема операций монтирования томов.

Совет: Можно столкнуться с ожиданием монтирования, или оно может занимать больше времени, чем обычно, когда включено совместное размещение по файловым пространствам и на узле есть том, содержащий несколько файловых пространств. Если том подлежит приему данных, IBM Spectrum Protect будет ждать этого тома.

Совместное размещение пулов хранения копий

Применение функции совместного размещения для пулов хранения копий должно осуществляться с особой осторожностью. Совместное размещение пулов хранения копий, особенно на узле или в файловом пространстве, приводит к увеличению числа частично заполненных томов, а также к выполнению потенциально ненужных операций освобождения пространства.

Первичные пулы хранения выполняют роль в восстановлении, отличающуюся от пулов хранения копий. Обычно вы используете первичные пулы хранения для восстановления данных непосредственно на клиентах. В случае серьезной аварии, когда выходят из строя и клиенты, и сервер, можно использовать тома пулов хранения копий вне площадки для восстановления

первичных пулов хранения. Типы сценариев восстановления могут помочь определить, использовать ли совместное размещение в пулах хранения копий.

Обычно большое количество частично заполненных томов появляется при совместном размещении на уровне узлов или файловых пространств. Однако при совместном размещении на уровне групп этот эффект проявляется незначительно. Наличие частично заполненных томов приемлемо для первичных пулов хранения, поскольку такие тома остаются доступными и могут заполняться новыми данными в ходе следующих процессов переноса. Однако частично заполненные тома могут быть неприемлемы для пулов хранения копий, тома пулов хранения которых сразу переводятся в автономный режим. Если вы решите применять совместное размещение для пулов хранения копий, вы окажетесь перед следующим выбором:

- Хранить большее количество частично заполненных томов автономно, увеличивая тем самым частоту операций освобождения пространства, когда снижается или достигается порог высвобождения томов.
- Оставлять частично заполненные тома подключенными до тех пор, пока они не заполнятся, рискуя утратить их в случае серьезной аварии и в результате не иметь возможности восстановить содержащиеся на них данные;
- Или осуществлять совместное размещение на уровне групп, чтобы использовать максимально возможную емкость ленточных устройств.

Если совместное размещение выключено для пула хранения копий, после резервного копирования данных в пул хранения копий, в нем как правило, остается всего несколько частично заполненных томов.

Внимательно изучите доступные опции перед использованием совместного размещения для пулов хранения, а также для принятия решения об использовании синхронной записи. Если синхронная запись не используется и вы используете совместное размещение для первичных пулов хранения, может потребоваться отключить совместное размещение для пулов хранения копий. Совместное размещение для пулов хранения копий может быть желательно при наличии нескольких клиентов, у каждого из которых каждый день возникает много данных инкрементного резервного копирования. Для совместного размещения с синхронной записью необходимо обеспечить, чтобы параметры совместного размещения были идентичны для первичных пулов хранения и пулов хранения копий.

Совместное размещение пулов длительного хранения

Значение, которое вы выбрали для свойства совместного размещения, влияет на то, как данные набора хранения распределяются по ленточным томам. В целом, чтобы использовать наименьшее число ленточных томов, совместное размещение должно быть отключено. По умолчанию параметр совместного размещения для пулов длительного хранения отключен.

При отключенном параметре совместного размещения при выборе тома для процессов копирования наборов хранения сервер пытается использовать все доступное пространство на каждом ленточном томе, прежде чем выбрать новый том. В то время как этот процесс обеспечивает более эффективное использование отдельных ленточных томов, данные для каждого набора хранения не размещаются совместно и могут быть распределены по многим ленточным томам.

Ваши параметры совместного размещения могут значительно повлиять на производительность системы, когда данные набора хранения записываются на ленту и производительность системы во время операций для восстановления данных набора хранения. Прежде чем вы рассмотрите, включить ли параметры совместного размещения для пулов длительного хранения, рассмотрите свои требования и компромиссы производительности.

- Если совместное размещение включено, сервер пытается хранить файлы для каждого объекта на минимальном числе ленточных томов. Однако эта опция увеличивает и время обработки на сервере, необходимое для размещения файлов для хранения, и количество требуемых томов. Учитывается также значение параметра **STACK**, заданное для этого набора хранения.

Совет: Если для набора хранения включена поддержка дополнения, данные этого набора хранения могут совместно использовать ленточные тома с данными, скопированные из других наборов хранения. При выборе тома сначала ищутся тома, находящиеся в состоянии ЗАПОЛНЕНИЕ и уже содержащие данные, но только если эти тома еще не используются в наборах хранения, требующих отдельного тома. Если для набора хранения не включено дополнение томов, такой набор хранения будет совместно размещаться на одном или нескольких ленточных томах, а данные из других наборов хранения в эти тома не записываются. При выборе тома ищутся пустые тома, но данные могут также копироваться в тома в состоянии ЗАПОЛНЕНИЕ, при условии, что эти тома уже содержат данные из копируемого набора хранения.

- Если возможность совместного размещения данных отключена, поскольку для отдельных наборов хранения могут распределяться по многим томам, возможно, потребуется больше монтирований ленты, если требуется восстановить данные набора хранения. Если требуется больше монтирования ленточных носителей, время обработки, необходимое для операций восстановления, может увеличиться.

Совет: Можно включить совместное размещение или изменить параметры совместного размещения, задав параметр **COLLOCATE** в командах **DEFINE STGPOOL** или **UPDATE STGPOOL**.

Изменение параметра совместного размещения влияет только на данные, которые записываются в пул длительного хранения после этого. Файлы, которые уже хранятся в пуле, не затрагиваются.

Понятия, связанные с данным

“Выбор томов с выключенным совместным размещением” на стр. 183

Когда функция совместного размещения отключена, сервер сначала пытается использовать все свободное пространство одного тома и лишь потом обращается к следующему тому.

“Влияние функции совместного размещения на выполнение операций” на стр. 179

Влияние функции совместного размещения на ресурсы и производительность системы зависит от типа выполняемых операций.

Планирование применения и активизация функции совместного размещения

Имея представление о результатах применения совместного размещения, можно сократить число операций монтирования носителей, более рационально использовать пространство на томах с последовательным доступом и повысить эффективность операций сервера.

Об этой задаче

Таблица 32 на стр. 186 содержит список четырех опций совместного размещения, которые можно задавать в командах **DEFINE STGPOOL** и **UPDATE STGPOOL**. В таблице указано также, как совместное размещение влияет на данные из узлов, принадлежащих и не принадлежащих группам совместного размещения.

Таблица 32. Опции совместного размещения и их воздействие на данные узлов

Опция совместного размещения	Узел не является членом ни одной группы совместного размещения	Узел является членом одной из групп совместного размещения
Нет	Для данных этого узла совместное размещение не применяется.	Для данных этого узла совместное размещение не применяется.
Группа	Сервер размещает данные узла на как можно меньшем числе томов в пуле хранения.	Сервер размещает данные узла и других узлов из той же группы совместного размещения на как можно меньшем числе томов
Узел	Сервер размещает данные узла на как можно меньшем числе томов.	Сервер размещает данные узла на как можно меньшем числе томов.

Таблица 32. Опции совместного размещения и их воздействие на данные узлов (продолжение)

Опция совместного размещения	Узел не является членом ни одной группы совместного размещения	Узел является членом одной из групп совместного размещения
File space	Сервер размещает данные узла на как можно меньшем числе томов. Если узел имеет несколько файловых пространств, сервер сохраняет их данные на разных томах	Сервер размещает данные узла на как можно меньшем числе томов. Если узел имеет несколько файловых пространств, сервер сохраняет их данные на разных томах

Таблица 33. Опции групп совместного размещения и влияние на данные файлового пространства

Опция совместного размещения	Если файловое пространство не определено как участник группы совместного размещения	Если файловое пространство определено как участник группы совместного размещения
Нет	Данные для файлового пространства совместно не размещаются.	Данные для файлового пространства совместно не размещаются.
Группа	Сервер размещает данные файлового пространства на как можно меньшем числе томов в пуле хранения.	Сервер сохраняет данные для файлового пространства и других файловых пространств, принадлежащих к той же группе совместного размещения, в возможно меньшем числе томов.
Узел	Сервер размещает данные узла на как можно меньшем числе томов.	Сервер размещает данные узла на как можно меньшем числе томов.
File space	Сервер размещает данные узла на как можно меньшем числе томов. Если узел имеет несколько файловых пространств, сервер сохраняет их данные на разных томах	Сервер сохраняет данные для файловых пространств в возможно меньшем числе томов. Если узел имеет несколько файловых пространств, сервер сохраняет их данные на разных томах

Процедура

Решая, стоит ли и как именно осуществлять совместное размещение данных, сделайте следующее:

1. Определите, как следует организовать данные: на основе узлов клиентов, на основе группы узлов клиентов или на основе файловых пространств. Для совместного размещения по группам нужно решить, как сгруппировать узлы:
 - Если целью является экономия пространства, объединение маленьких узлов в одну группу позволит экономнее использовать ленты.
 - Если целью является потенциальное ускорение клиентских операций восстановления, сгруппируйте вместе узлы, чтобы они заполняли максимально возможное число лент. Если сгруппировать узлы вместе, данные отдельных узлов будут распределены по двум или более лентам и одновременно можно будет смонтировать больше лент во время операции восстановления без запроса в нескольких сеансах.
 - Если целью является разделение данных по отделам, можно группировать узлы по отделам.
2. Чтобы произвести совместное размещение групп, выполните следующие шаги:
 - а) Задайте группы совместного размещения с помощью команды **DEFINE COLLOGROUP**.
 - б) Добавьте в группы совместного размещения клиентские узлы с помощью команды **DEFINE COLLOCMEMBER**.

В организации совместного размещения на уровне групп вам помогут следующие запросы:

QUERY COLLOGROUP

Показывает группы совместного размещения, заданные на сервере.

QUERY NODE

Позволяет вызвать на экран имя группы совместного размещения, к которой принадлежит заданный узел.

QUERY NODEDATA

Позволяет вызвать на экран информацию о данных для одного или более узлов в пуле хранения с последовательным доступом.

QUERY STGPOOL

Позволяет вызвать на экран информацию о размещении клиентских данных в пуле хранения с последовательным доступом и объеме пространства, занятого на томе данными одного узла.

Также можно использовать сценарии сервера IBM Spectrum Protect или сценарии PerlL, чтобы увидеть информацию, которая может оказаться полезной при создании определений групп совместного размещения.

3. Укажите, как следует производить совместное размещение данных в пуле хранения, введя команду **DEFINE STGPOOL** или **UPDATE STGPOOL** с параметром **COLLOCATE**.

Дальнейшие действия

Подсказка: Чтобы сократить число операций монтирования носителей, более эффективно использовать пространство на последовательных томах и включить совместное размещение, выполните следующие шаги:

- Определить иерархию пулов хранения и политику с требованием, чтобы эти резервные, архивные файлы и файлы с управлением пространством изначально хранились в дисковых пулах хранения.

Осуществляя перенос данных из дискового пула хранения, сервер выбирает клиентский узел или группу совместного размещения, данные которых занимают в этом пуле хранения больше всего пространства, и пытается перенести все файлы этого узла или группы. Этот процесс хорошо совместим с функцией совместного размещения, поскольку сервер старается поместить все файлы конкретного клиента или их группы на один том с последовательным доступом.

- Разрешите для пула хранения с последовательным доступом использование чистых томов, чтобы сервер мог выбирать новые тома для совместного размещения данных.
- Задайте клиентскую опцию COLLOCATEBYFILESPEC, чтобы ограничить количество лент, на которые записываются объекты, связанные с одной спецификацией файла. Эта опция позволяет более эффективно осуществлять совместное размещение на уровне серверов; она не заменяет установку совместного размещения на уровне файловых пространств или групп.

Управление ленточными устройствами

Стандартные операции с лентами включают подготовку ленточных томов для использования, управления, как и когда тома используются снова, и обеспечение, что доступно достаточно томов. Надо также отвечать на запросы, адресованные оператору, и управлять библиотеками, накопителями, дисками, путями и устройствами перемещения данных.

Подготовка сменных носителей

Прежде чем съемный носитель можно будет использовать для хранения данных, его надо подготовить. Стандартные операции подготовки включают определение меток томов и регистрацию томов.

Об этой задаче

Когда IBM Spectrum Protect обращается к тому на сменном носителе, он проверяет имя тома в заголовке его метки, чтобы гарантировать получение доступа к нужному тому.

Ленточным томам следует присваивать метки для того, чтобы сервер мог их использовать.

Процедура

Чтобы подготовить том для использования, выполните следующие действия:

1. Присвойте метку тому, используя команду **LABEL LIBVOLUME**.
2. При использовании автоматизированных библиотек необходимо включить том в библиотеку. Инструкции смотрите в разделе [“Регистрация томов в автоматизированной библиотеке”](#) на стр. 191,

Подсказка: При использовании команды **LABEL LIBVOLUME** с накопителями автоматизированной библиотеки можно снабдить тома метками и включить их в библиотеку одной командой.

3. Если данный пул хранения не может содержать чистых томов (**MAXSCRATCH=0**), то определите том для IBM Spectrum Protect по имени, чтобы позже к нему можно было осуществлять доступ.

Если пул хранения может содержать чистые тома (для параметра **MAXSCRATCH** указано значение, не равное нулю), то пропустите этот шаг.

Запись меток томов на ленточных томах

Ленточные тома следует снабжать метками до их определения для сервера.

Об этой задаче

Для автоматизированных библиотек выводится приглашение вставить том в слот входа/выхода библиотеки. Если доступной станции ввода-вывода нет, то вставьте том в пустой слот. Томам можно присвоить метки, когда вы их будете активировать или до их активирования.

Процедура

Чтобы присвоить томам метки до их активации, выполните следующие шаги:

1. Присвойте метки ленточным томам, используя команду **LABEL LIBVOLUME**. Например, чтобы присвоить имя **VOLUME1** тому в библиотеке **LIBRARY 1**, введите следующую команду:

```
label libvolume library1 volume1
```

Требование: Должен быть доступен хотя бы один накопитель. Накопитель не может использоваться другим процессом IBM Spectrum Protect. Если том бездействует, то накопитель считается недоступным.

2. Чтобы перезаписать существующие метки томов, укажите параметр **OVERWRITE=YES**. По умолчанию команда **LABEL LIBVOLUME** не перезаписывает текущую метку тома.

Задачи, связанные с данной

Присвоение меток новым томам с использованием **AUTOLABEL**

Использование параметра **AUTOLABEL** в команде **DEFINE LIBRARY** или **UPDATE LIBRARY** более эффективно, чем использование команды **LABEL LIBVOLUME**, которая требует, чтобы тома монтировались по отдельности.

Информация, связанная с данной

[LABEL LIBVOLUME \(запись метки на том библиотеки\)](#)

Запись меток томов в SCSI библиотека

Томам можно присваивать метки по отдельности, или можно использовать IBM Spectrum Protect, чтобы произвести поиск томов в библиотеке и присвоить метки найденным томам.

Маркировка томов по отдельности

Когда вы маркируете тома по отдельности при помощи команды **LABEL LIBVOLUME**, надо указать имя тома.

Процедура

1. Вставьте тома во входной/выходной слот библиотеки, когда сервер предложит вам это. Библиотека монтирует каждый вставленный том в накопитель.
2. При использовании библиотеки SCSI введите имя тома, когда вам это предложат. Метка с указанным именем будет записана в том.

Совет: Чтобы у вас запросили имя тома для библиотеки SCSI, введите команду **LABEL LIBVOLUME** и задайте параметр **LABELSOURCE=PROMPT**.

3. Если у библиотеки нет входного/выходного порта, вам предложат извлечь ленту из слота с указанным номером. Удалите ленту из указанного слота.
Если библиотек имеет порт входа/выхода, то эта команда по умолчанию возвращает каждый помеченный том в этот порт.

Перезапись меток томов в библиотеке SCSI

При помощи команды **LABEL LIBVOLUME** можно перезаписать существующие метки томов, если на томах хранения нет действительных данных.

Об этой задаче

Томам в библиотеке SCSI можно присвоить метки, даже если у них нет входного/выходного порта. После того как будут записаны метки томов, нужно вручную вставить каждый новый том в библиотеку и поместить тома в слоты хранения в библиотеке.

Процедура

Перезапишите существующие метки томов, введя команду **LABEL LIBVOLUME**. Например, если имя библиотеки - LIB1, а имя тома - VOLNAME, введите следующую команду:

```
label libvolume lib1 volname overwrite=yes
```

Присвоение меток новым томам с использованием AUTOLABEL

Использование параметра **AUTOLABEL** в команде **DEFINE LIBRARY** или **UPDATE LIBRARY** более эффективно, чем использование команды **LABEL LIBVOLUME**, которая требует, чтобы тома монтировались по отдельности.

Процедура

Введите команду **DEFINE LIBRARY** или **UPDATE LIBRARY**, задав опцию **AUTOLABEL**.

Совет: Если параметр **AUTOLABEL** используется при работе с библиотекой SCSI, то необходимо зарегистрировать ленты, указав параметр **CHECKLABEL=BARCODE** в команде **CHECKIN LIBVOLUME**. Значение параметра **AUTOLABEL** по умолчанию - NO для всех библиотек SCSI и YES для всех остальных библиотек. Параметр **CHECKLABEL=BARCODE** учитывается, только если в библиотеке есть устройство для считывания штрих-кода.

Информация, связанная с данной

[CHECKIN LIBVOLUME \(регистрация тома хранения в библиотеке\)](#)

[DEFINE LIBRARY \(Задать библиотеку\)](#)

[LABEL LIBVOLUME \(запись метки на том библиотеки\)](#)

Выбор библиотеки и запись меток томов

IBM Spectrum Protect может производить поиск по всем слотам портов с целью нахождения томов и может попытаться присвоить метку каждому найденному тому.

Процедура

Чтобы произвести поиск в библиотеке и присвоить томам метки, введите команду **LABEL LIBVOLUME** и задайте параметр **SEARCH=YES**.

Совет: Если библиотека SCSI оснащена устройством для считывания штрих-кода, то команда **LABEL LIBVOLUME** использует его для получения имен томов и не запрашивает их у пользователя. Параметр **LABELSOURCE=BARCODE** применим только для библиотек SCSI.

Например, чтобы присвоить метки всем томам в библиотеке SCSI, введите следующую команду:

```
label libvolume имя_библиотеки search=yes labelsource=barcode
```

IBM Spectrum Protect выберет следующий доступный накопитель, так что вы сможете продолжить поиск.

Результаты

После записи метки том возвращается в исходное расположение в библиотеке.

Информация, связанная с данной

[LABEL LIBVOLUME \(запись метки на том библиотеки\)](#)

Регистрация томов в автоматизированной библиотеке

Вы можете активировать том в автоматизированной библиотеке, используя команду **CHECKIN LIBVOLUME**.

Прежде чем начать

Чтобы автоматически присвоить лентам метки до их активации, введите команду **DEFINE LIBRARY**, задав параметр **AUTOLABEL=YES**. Используя параметр **AUTOLABEL**, вы избежите необходимости предварительно задавать метку для набора лент.

Об этой задаче

Каждый том, используемый сервером в каких бы то ни было целях, должен иметь уникальное имя. Это требование относится ко всем томам, независимо от того, используются ли они для пулов хранения или таких операций, как экспорт или резервное копирование базы данных. Требование относится также к томам, находящимся в разных библиотеках, но используемых одним сервером.

Советы:

- Не используйте одну библиотеку для томов со штрих-кодowymi метками и томов, у которых нет таких меток. Сканирование штрих-кодов может занять длительное время для непомеченных томов.
- Для сервера допустимы только ленты со стандартными метками IBM.
- Все тома, штрих-код которых начинается с CLN, рассматриваются как чистящая лента.
- Если для тома есть запись в файле хронологии, его нельзя зарегистрировать как чистый том.

Процедура

1. Чтобы активировать том хранения в библиотеке, введите команду **CHECKIN LIBVOLUME**.

Совет: Команда всегда выполняется как фоновый процесс. Дождитесь завершения выполнения процесса **CHECKIN LIBVOLUME**, прежде чем задавать тома, иначе этот процесс завершится неудачно. Можно сэкономить время, выполняя регистрацию томов как часть операции маркировки.

2. Присвойте библиотеке имя и укажите, является ли том закрытым или чистым. В зависимости от используемых томов (чистые или закрытые) выполните одно из следующих действий.
 - Если используются только чистые тома, убедитесь в доступности достаточного количества чистых томов. Например, может потребоваться пометить дополнительные тома. Кроме того, после начала использования томов может понадобиться увеличить количество чистых

томов, разрешенных для использования пулом хранения, определенным для данной библиотеки.

- Если в библиотеке необходимо использовать закрытые тома в дополнение к чистым томам или вместо них, задайте тома в пуле хранения, используя команду **DEFINE VOLUME**. Вы должны пометить и активировать заданные вами тома.

Задачи, связанные с данной

Запись меток томов на ленточных томах

Ленточные тома следует снабжать метками до их определения для сервера.

Активация одного тома в библиотеке SCSI

Можно активировать один том, введя команду **CHECKIN LIBVOLUME** и задав параметр **SEARCH=NO**. IBM Spectrum Protect попросит оператора монтирования загрузить том во входной/выходной слот в библиотеке.

Процедура

1. Введите команду **CHECKIN LIBVOLUME**.

Например, чтобы активировать том VOL001, введите следующую команду:

```
checkin libvolume tapelib vol001 search=no status=scratch
```

2. Отреагируйте на подсказку с сервера.

- Если библиотека имеет порт входа/выхода, то выводится приглашение вставить ленту в порт входа/выхода.
- Если библиотека не имеет порта входа/выхода, то выводится приглашение вставить ленту в один из слотов библиотеки. Адреса элементов позволяют идентифицировать эти слоты. Например, сервер обнаруживает, что первый пустой слот - это слот с адресом элемента, равным 5. В этом случае сообщение будет выглядеть следующим образом:

```
ANR8306I 001: Вставьте том 8MM VOL001 R/W в слот с адресом элемента
5 библиотеки TAPELIB в течение 60 минут; введите команду 'REPLY' вместе
с идентификатором запроса, когда будете готовы.
```

Если вы не знаете, где находится в библиотеке элемент с адресом 5, смотрите рабочую таблицу для устройства. Чтобы найти рабочую таблицу, смотрите документацию по вашей библиотеке. Вставив том (в ответ на соответствующее предложение), ответьте на сообщение от клиента администрирования IBM Spectrum Protect. Введите команду **REPLY**, указав после нее номер требования (номер в начале требования о монтировании), например:

```
reply 1
```

Совет: Иногда адреса элементов нумеруются, начиная с номера, отличного от единицы. Чтобы точно узнать нумерацию, смотрите рабочую таблицу. Если на сайте [IBM для IBM Spectrum Protect](#) отсутствует рабочая таблица для вашего устройства, смотрите документацию по вашей библиотеке.

Если вы зададите время ожидания, равное 0, используя дополнительный параметр **WAITTIME** в команде **CHECKIN LIBVOLUME**, команда **REPLY** не потребуется. Время ожидания по умолчанию составляет 60 минут.

Регистрация томов в слотах хранения библиотеки

Если у вас много томов, которые нужно активировать, и вы не хотите вводить команду **CHECKIN LIBVOLUME** для каждого тома, вы можете произвести поиск слотов хранения для новых томов. Сервер найдет тома, которые еще не были добавлены в перечень.

Процедура

1. Откройте библиотеку и поместите новые тома в неиспользуемые слоты.

Например, в случае устройства SCSI откройте дверцу библиотеки, вставьте все новые тома в незанятые слоты и закройте дверцу.

2. Если томам не присвоены метки, используйте команду **LABEL LIBVOLUME**, чтобы присвоить тому метку.
3. Выполните команду **CHECKIN LIBVOLUME** с параметром **SEARCH=YES**.

Информация, связанная с данной

CHECKIN LIBVOLUME (регистрация тома хранения в библиотеке)

Активация томов со входных и выходных портов библиотеки

Вы можете произвести поиск промаркированных томов во всех слотах входных и выходных портов, и сервер может активировать их автоматически.

Прежде чем начать

Введите команду **LABEL LIBVOLUME**, чтобы присвоить метки томам, у которых их еще нет.

Об этой задаче

При работе с библиотеками SCSI сервер проверяет все порты входа/выхода библиотеки на наличие томов. При обнаружении тома с действительной меткой он активируется автоматически.

Процедура

Введите команду **CHECKIN LIBVOLUME** с параметром **SEARCH=BULK**.

- Чтобы загрузить ленту в накопитель и прочесть метку, задайте параметр **CHECKLABEL=YES**. После того как сервер прочесть метку, он переместит ленту из накопителя в слот хранения.
- Чтобы сервер использовал устройство для чтения штрих-кода для проверки внешних меток на лентах, задайте параметр **CHECKLABEL=BARCODE**. Когда включено чтение штрих-кода, сервер читает метку и перемещает ленту со входного/выходного порта в слот хранения.

Активация томов с использованием устройств чтения штрих-кода

При активации томов в библиотеках, снабженных устройствами чтения штрих-кода, можно сэкономить время, используя символы на этикетках со штрих-кодом в качестве имен томов.

Об этой задаче

Сервер читает метки со штрих-кодом и использует эту информацию для записи внутренних меток носителей. В случае томов, у которых нет этикеток со штрих-кодом, сервер монтирует тома в накопитель и пытается прочесть внутреннюю записанную метку.

Процедура

Введите команду **CHECKIN LIBVOLUME** с параметром **CHECKLABEL=BARCODE**.

Например, чтобы с помощью устройства считывания штрих-кода выполнить поиск в библиотеке с именем TAPELIB и зарегистрировать чистую ленту, введите следующую команду:

```
checkin libvolume tapelib search=yes status=scratch checklabel=barcode
```

Регистрация томов с использованием устройств чтения штрих-кода

Вы сможете сэкономить время при активации томов, используя устройство чтения штрих-кода, если оно есть в библиотеке.

Об этой задаче

При активации тома можно указать, надо ли считывать метки носителей во время активации. Если проверка метки включена, IBM Spectrum Protect монтирует каждый том, чтобы считать внутреннюю метку, и активирует том, только если он должным образом помечен. Проверка меток

поможет в будущем предотвратить ошибки, когда тома будут использоваться в пулах хранения, но при этом время обработки регистрации увеличивается.

Если том не имеет этикетки со штрих-кодом, то IBM Spectrum Protect монтирует его в накопитель и пытается считать записанную метку.

Процедура

Чтобы активировать тома, используя устройство считывания штрих-кода, введите команду **CHECKIN LIBVOLUME**, задав параметр **CHECKLABEL=BARCODE**. Например, чтобы с помощью устройства считывания штрих-кода активировать все тома как чистые тома в библиотеке TAPELIB, введите следующую команду:

```
checkin libvolume tapelib search=yes status=scratch checklabel=barcode
```

Задачи, связанные с данной

Подготовка сменных носителей

Прежде чем съемный носитель можно будет использовать для хранения данных, его надо подготовить. Стандартные операции подготовки включают определение меток томов и регистрацию томов.

Информация, связанная с данной

CHECKIN LIBVOLUME (регистрация тома хранения в библиотеке)

Активация томов в полной библиотеке с заменой

Если при активации томов в библиотеке отсутствуют пустые слоты, то активация завершится неудачно, если не будет разрешена замена томов. Если вы включите замену, а библиотека окажется заполнена, сервер выберет том, который нужно извлечь, а затем активирует затребованный вами том.

Об этой задаче

Сервер выберет том, который нужно извлечь, проверив сначала наличие любого доступного чистого тома, а затем тома, который монтировался реже других. Сервер удалит выбранный для замены том из библиотеки и заменит его томом, который вы активируете.

Процедура

- Чтобы заменять тома, если пустой слот библиотеки недоступен для активации тома, введите команду **CHECKIN LIBVOLUME**, задав параметр **SWAP=YES**.
Например, чтобы активировать том с именем VOL1 в библиотеке AUTO и задать замену, введите следующую команду:

```
checkin libvolume auto vol1 swap=yes
```

Задачи, связанные с данной

Управление заполненной библиотекой с хранилищем переполнения

С ростом потребности в пространстве хранения число томов, необходимых в пуле хранения, может превысить физическую емкость автоматизированной библиотеки. Чтобы сделать пространство доступным для новых томов и чтобы отслеживать существующие тома, можно задать систему хранения переполнения для пула хранения.

Информация, связанная с данной

CHECKIN LIBVOLUME (регистрация тома хранения в библиотеке)

Закрытые и чистые тома

Чтобы оптимизировать хранение на ленте, прочтите информацию о закрытых томах и чистых томах. Используйте закрытые тома и чистые тома соответствующим образом.

Закрытые тома не могут быть перезаписаны, если запрошено монтирование чистых томов. Активировать том в состоянии Чистый нельзя, если этот том используется пулом хранения для

экспорта данных, для резервного копирования базы данных или для резервного копирования на том набора резервных копий.

Частично записанные тома всегда являются закрытыми. Тома имеют состояние либо чистых, либо закрытых, но когда IBM Spectrum Protect сохраняет на них данные, их состояние становится закрытым.

Таблица 34. Использование закрытых томов и чистых томов	
Тип тома	Когда следует использовать
Закрытые тома	Используйте закрытые тома, чтобы контролировать тома, используемые отдельными пулами хранения, и вручную управлять томами. Чтобы задать закрытые тома, введите команду DEFINE VOLUME . Для восстановления базы данных, дампа памяти или загрузки, а также для серверных операций импорта нужно указать закрытые тома.
Свободные тома	<p>В некоторых случаях можно упростить управление томами, используя чистые тома. Чистые тома можно использовать в следующих случаях:</p> <ul style="list-style-type: none">• Когда не нужно описывать каждый том в пуле хранения.• Если вы хотите воспользоваться преимуществами автоматизации роботизированных устройств.• Когда разные пулы хранения совместно используют автоматизированную библиотеку, и пулы хранения могут динамически получить тома из чистых томов в библиотеке. Предварительно распределять тома по пулам хранения не требуется.

Задачи, связанные с данной

[Изменение состояния тома в автоматизированной библиотеке](#)

Вы можете изменить состояние тома с private (закрытый) на scratch (чистый) или наоборот.

Информация, связанная с данной

[CHECKIN LIBVOLUME \(регистрация тома хранения в библиотеке\)](#)

[DELETE VOLUME \(удаление тома пула хранения\)](#)

Адреса элементов для слотов хранения в библиотеке

Адрес элемента — это номер, который указывает физическое размещение слота системы хранения или накопителя в автоматизированной библиотеке.

Если в библиотеке есть входные/выходные порты, вы можете добавлять и удалять носители, используя порты. Если никаких входных/выходных портов нет, вы должны будете загрузить ленты в слоты хранения.

Если вы загружаете ленточные носители в слоты хранения, вы должны должны будете реагировать на запросы о монтировании, в которых слоты системы хранения будут указаны в виде адресов элементов. Если при вводе команды **CHECKIN LIBVOLUME** или **LABEL LIBVOLUME** вы не задали нулевое время ожидания, вам не нужно будет реагировать на требование монтирования.

Адреса элементов смотрите в документации производителя устройства или перейдите на сайт [IBM для IBM Spectrum Protect](#) и произведите поиск адресов элементов.

Информация, связанная с данной

[CHECKIN LIBVOLUME \(регистрация тома хранения в библиотеке\)](#)

[LABEL LIBVOLUME \(запись метки на том библиотеки\)](#)

Управление перечнем томов

Перечнем томов можно управлять, контролируя доступ сервера к томам, повторно используя ленты, а также повторно используя тома для операций резервного копирования базы данных и экспорта. Перечнем также можно управлять, поддерживая запас чистых томов.

Об этой задаче

Каждый том, использующийся сервером, должен иметь уникальное имя, независимо от того, используются ли они для пулов хранения или таких операций, как экспорт или резервное копирование базы данных. У томов, находящихся в разных библиотеках, но используемых одним и тем же сервером, также должны быть уникальные имена.

Управление доступом к томам

Для управления доступом к томам можно использовать разные методы.

Процедура

Чтобы управлять доступом к томам, выполните любое из следующих действий:

- Чтобы запретить серверу монтировать том, введите команду **UPDATE VOLUME** и задайте параметр **ACCESS=UNAVAILABLE**.
- Чтобы сделать тома недоступными и отправить их куда-либо вне площадки для защиты, используйте пул хранения копий или пул хранения активных данных.
- Можно создать резервные копии первичных пулов хранения, после чего отправить тома пула хранения копий в удаленную систему хранения.
- Можно скопировать активные версии клиентских резервных данных в пулы хранения активных данных, а затем отправить тома в систему хранения, расположенную вне узла.
- Отслеживать тома пула хранения копий и пула активных данных можно путем изменения режима доступа к ним на доступ вне площадки, а также путем обновления журнала томов для определения их расположения.

Информация, связанная с данной

[UPDATE VOLUME \(изменение тома пула хранения\)](#)

Повторное использование лент

Чтобы поддерживать необходимый запас лент, вы можете производить удаление устаревших файлов, освобождать тома и удалять тома, срок службы которых подошел к концу. Вы также можете держать в запасе чистые тома.

Об этой задаче

Со временем носители устаревают, а размещенные на них резервные копии данных становятся ненужными. Можно задать политики сервера, определяющие количество версий резервных копий и срок их хранения. Можно использовать обработку устаревания, чтобы удалять файлы, которые вам больше не нужны. Нужные вам данные можно оставить на носителе. Когда данные станут вам больше не нужны, вы сможете высвободить носители и использовать их повторно.

Процедура

1. Удаляйте ненужные данные клиента, регулярно выполняя обработку устаревания. При обработке устаревания удаляются данные, которые устарели либо в результате превышения

срока хранения, указанного в политике, либо потому, что администратор удалил активные версии данных.

2. Повторно используйте тома в пулах хранения, выполняя обработку освобождения.

В процессе обработки освобождения носителей все не устаревшие данные перемещаются с многих томов на меньшее количество томов. После этого носители могут быть возвращены в пул хранения и использованы повторно.

3. Повторно используйте тома, содержащие устаревшие резервные копии базы данных или ненужные экспортированные данные, удаляя хронологию томов.

Прежде чем сервер сможет повторно использовать тома, отслеживаемые в файле хронологии томов, вы должны удалить информацию о томе из файла хронологии томов, введя команду **DELETE VOLHISTORY**.

Совет: Если сервер использует disaster recovery manager (DRM), то информация о томах удаляется автоматически во время обработки команды **MOVE DRMEDIA**.

4. Определяйте, какие ленточные тома достигают окончания срока использования. Сервер можно использовать для вывода статистики томов, включающей в себя число операций записи, выполненных на носитель, и число ошибок записи. Для закрытых и чистых томов будут показаны следующие статистические данные:

Закрытые тома

Для носителей, изначально определенных как закрытые тома, сервер сохраняет статистические данные, даже когда том освобождается. Эту информацию можно сравнить с количеством операций записи и ошибок записи, рекомендованным производителем.

Свободные тома

Для носителей, изначально определенных в качестве чистых томов, сервер обновляет статистические данные при каждом освобождении томов.

5. Следует восстановить все действительные данные с томов, достигших окончания срока использования. Если тома находятся в автоматизированных библиотеках, следует отменить их регистрацию в перечне библиотеки. Удалите закрытые тома из базы данных при помощи команды **DELETE VOLUME**.
6. Убедитесь, что тома доступны для ротации лент, и пулу хранения не грозит нехватка пространства. Для мониторинга доступности чистых томов можно использовать Центр операций. Убедитесь, что число чистых томов достаточно велико, чтобы соответствовать требованиям. Дополнительную информацию смотрите в разделе [“Поддержание запаса томов в библиотеке, содержащей носители WORM”](#) на стр. 199.

носитель WORM: Накопители однократной записи и многократного чтения (Write Once Read Many, WORM) при отмене сервером транзакций могут зря расходовать носители, поскольку тома становятся недоступными для выполнения резервного копирования. После того, как сервер произведет запись на тома WORM, пространство на томе нельзя будет использовать повторно, даже если транзакции были отменены (например, при отмене резервного копирования из-за недостаточного числа носителей в устройстве). Чтобы свести к минимуму бесполезное расходование носителей WORM, сделайте следующее:

- а. Убедитесь, что максимальное количество чистых томов для пула хранения устройства как минимум равно количеству слотов системы хранения в библиотеке.
- б. Зарегистрируйте в перечне томов устройства достаточное количество томов для ожидаемой загрузки.

Если большинство операций резервного копирования предназначено для небольших файлов, то управление размером транзакций может повлиять на использование дисков WORM. Чем меньше операция, тем меньшее количество места становится непригодным в случае отмены операции (например, резервного копирования). Размеры операций управляются серверным параметром TXNGROUPMAX и клиентским параметром TXNBYTELIMIT.

Задачи, связанные с данной

[Перенос данных на обновленные накопители](#)

Если вы обновляете все ленточные накопители в библиотеке, вы можете сохранить существующие определения правил политики, чтобы производить перенос и удаление устаревших существующих данных, и сможете использовать новые накопители для сохранения данных.

Управление серверными запросами на тома

IBM Spectrum Protect показывает требования и сообщения о состоянии во всех клиентах командой строки администрирования, запущенных в режиме консоли. Часто эти запросы ограничены по времени. Успешные операции сервера должны быть выполнены в рамках заданного предела времени; в противном случае произойдет тайм-аут операции.

Информация, связанная с данной

DELETE VOLHISTORY (Удалить информацию хронологии томов с последовательным доступом)

DELETE VOLUME (удаление тома пула хранения)

EXPIRE INVENTORY (ручной запуск обработки устаревания перечня)

RECLAIM STGPOOL (Освобождение томов пула хранения с последовательным доступом)

Опция Txnbytelimit

опция сервера TXNGROUPMAX

Поддержание запаса чистых томов.

Вы должны задать для пула хранения достаточно большое максимальное число чистых томов в соответствии с ожидаемым уровнем использования.

Об этой задаче

При задании пула хранения необходимо указать максимальное число свободных томов, которые может использоваться в пуле хранения. Сервер при необходимости запрашивает свободный том автоматически. Если число чистых томов, используемых сервером для пула хранения, превысит заданный максимум, это может привести к нехватке пространства в пуле хранения.

Процедура

Если пулу хранения потребуется число чистых томов, превышающее максимальное, можно выполнить одно из указанных ниже действий или оба эти действия:

1. Увеличьте максимальное количество чистых томов, введя команду **UPDATE STGPOOL** с параметром **MAXSCRATCH**.
2. Сделать тома доступными для повторного использования, запустив обработку устаревания и освобождения томов, чтобы собрать данные на меньшем числе томов.
 - a) Введите команду **EXPIRE INVENTORY**, чтобы запустить обработку устаревания.

Совет: По умолчанию этот процесс автоматически запускается каждый день. В файле серверных опций, `dsmserv.opt`, также можно задать серверную опцию **EXPINTERVAL**, чтобы автоматически запустить обработку устаревания. Значение, равное 0, указывает, что для запуска обработки устаревания нужно ввести команду **EXPIRE INVENTORY**.

- b) Введите команду **RECLAIM STGPOOL**, чтобы запустить обработку освобождения пространства.

Совет: Вы также можете задать пороги освобождения пространства, когда будете задавать пул хранения с использованием команды **DEFINE STGPOOL** с параметром **RECLAIMPROCESS**.

Дальнейшие действия

Если вам потребуется больше томов для будущих операций восстановления, присвойте метки дополнительным чистым томам, используя команду **LABEL LIBVOLUME**.

Задачи, связанные с данной

Поддержание запаса чистых томов в автоматизированной библиотеке

Задавая пул хранения, связанный с автоматизированной библиотекой, вы можете указать максимальное число чистых томов, равное физической емкости библиотеки. Если сервер

использует для пула хранения большее число чистых томов, вы должны убедиться, что у вас есть достаточное число доступных томов.

Информация, связанная с данной

[EXPIRE INVENTORY](#) (ручной запуск обработки устаревания перечня)

[LABEL LIBVOLUME](#) (запись метки на том библиотеки)

[RECLAIM STGPOOL](#) (Освобождение томов пула хранения с последовательным доступом)

[UPDATE STGPOOL](#) (обновить пул хранения)

Поддержание запаса томов в библиотеке, содержащей носители WORM

Предотвращайте отмену транзакций сохранения данных в библиотеках, содержащих тома с однократной записью и многократным чтением (Write-Once, Read-Many, WORM), поддерживая запас чистых или новых закрытых томов в библиотеке. Отмена транзакций может привести к бесполезному расходованию носителей WORM.

Об этой задаче

IBM Spectrum Protect отменяет транзакцию, если тома - закрытые или чистые - недоступны для завершения операции сохранения данных. После того как IBM Spectrum Protect начнет транзакцию, производя запись на том WORM, записанное на нем пространство нельзя будет использовать повторно даже в случае отмены транзакции.

Например, у вас есть тома WORM по 2,6 ГБ каждый, и клиент запустит резервное копирование файла объемом 12 ГБ. Если IBM Spectrum Protect не может после заполнения четырех чистых томов получить пятый, то операция резервного копирования отменяется. Четыре тома, которые IBM Spectrum Protect уже заполнил данными, не могут использоваться повторно.

Чтобы свести к минимуму отмену транзакций, в библиотеке должно быть достаточно доступных томов для выполнения ожидаемых операций клиентов (например, резервного копирования).

Процедура

1. Убедитесь, что в пуле хранения, связанном с библиотекой, достаточно чистых томов. Введите команду **UPDATE STGPOOL**, задав параметр **MAXSCRATCH**.
2. Чтобы управлять ожидаемой нагрузкой, активируйте в библиотеке достаточное количество чистых и закрытых томов, введя команду **CHECKIN LIBVOLUME**.
3. Чтобы управлять размером транзакций, задайте опцию сервера **TXNGROUPMAX** и опцию клиента **TXNBYTELIMIT**. Если клиент чаще сохраняет небольшие файлы, управление размером транзакций может повлиять на то, как используются тома WORM. Чем меньше транзакция, тем меньше пространства хранения будет израсходовано напрасно в случае отмены операции (например, резервного копирования).

Информация, связанная с данной

[CHECKIN LIBVOLUME](#) (регистрация тома хранения в библиотеке)

[UPDATE STGPOOL](#) (обновить пул хранения)

[Опция Txnbytelimit](#)

[опция сервера TXNGROUPMAX](#)

Управление перечнем томов в автоматизированных библиотеках

Сервер IBM Spectrum Protect использует перечень томов библиотеки для отслеживания чистых и закрытых томов, которые есть в автоматизированной библиотеке. Вы должны убедиться, что перечень соответствует томам, которые физически находятся в библиотеке.

Инвентарный список томов библиотеки отделен от инвентарного списка томов для каждого пула хранения. Чтобы добавить том в перечень томов библиотеки, вы активируете том в этой библиотеке IBM Spectrum Protect.

Список томов в перечне томов библиотеки может не совпадать со списком томов в перечне пулов хранения для устройства. Например, можно активировать чистые тома в библиотеке, но их нельзя

будет задан в пуле хранения. Если чистые тома не выбраны для резервного копирования, то вы сможете задать закрытые тома в пуле хранения, но не сможете активировать их в перечне томов для устройства.

Чтобы перечень томов для библиотеки сервера оставался точным, зарезервируйте тома, чтобы физически удалить тома из библиотеки SCSI. Если попытаться зарезервировать том, который используется в пуле хранения, том останется в пуле хранения. Если вы должны смонтировать том, когда он зарезервирован, на консоли оператора монтирования появится сообщение с требованием активировать том. Если операция активации завершится неудачно, сервер пометит том как недоступный.

Если том присутствует в перечне томов библиотеки, его можно перевести из состояния чистого в состояние закрытого.

Чтобы проверить, согласуется ли перечень томов библиотеки сервера с томами, физически находящимися в библиотеке, можно произвести аудит библиотеки. Перечень может стать неточным, если тома помещаются к библиотеку или удаляются из нее без передачи соответствующих сведений на сервер с помощью команд check-in или check-out.

Задачи, связанные с данной

Регистрация томов в автоматизированной библиотеке

Вы можете активировать том в автоматизированной библиотеке, используя команду **CHECKIN LIBVOLUME**.

Информация, связанная с данной

[AUDIT LIBRARY \(аудит томов автоматизированной библиотеки\)](#)

Изменение состояния тома в автоматизированной библиотеке

Вы можете изменить состояние тома с private (закрытый) на scratch (чистый) или наоборот.

Процедура

Чтобы изменить состояние тома, введите команду **UPDATE LIBVOLUME**.

Например, чтобы изменить состояние тома с именем VOL1 на частный том, введите следующую команду:

```
update libvolume lib1 vol1 status=private
```

ограничения:

- Если том принадлежит к пулу хранения или указан в файле хронологии томов, изменить состояние тома с закрытого на чистый нельзя.
- Закрытые тома должны представлять собой заданные администратором тома, на которых либо нет никаких данных, либо содержатся недействительные данные. Это не могут быть частично записанные тома, содержащие активные данные. При изменении состояния статистика тома теряется.

Удаление томов из автоматизированной библиотеки

Тома можно удалить из автоматизированной библиотеки, если вы экспортировали данные на том и хотите импортировать данные в другую систему. Вам также может потребоваться удалить тома, чтобы освободить место для новых томов.

Об этой задаче

По умолчанию сервер монтирует зарезервированный том и проверяет внутреннюю метку. При проверке метки сервер удаляет том из инвентарного списка томов библиотеки, а затем перемещает его на порт входа/выхода или на станцию ввода-вывода библиотеки. Если в библиотеке нет порта входа/выхода, то сервер выдает оператору монтирования запрос на удаление тома из слота в библиотеке.

Процедура

- Чтобы удалить том из автоматической библиотеки, введите команду **CHECKOUT LIBVOLUME**.
- Для автоматизированных библиотек с несколькими портами ввода/выхода введите команду **CHECKOUT LIBVOLUME** с параметром **REMOVE=BULK**. Сервер извлечет том к следующему доступному порту ввода/выхода.

Дальнейшие действия

Если вы резервируете том, заданный в пуле хранения, а серверу потребуется потом получить к нему доступ, то сервер затребует активацию тома. Чтобы вернуть тома в библиотеку, введите команду **CHECKIN LIBVOLUME**.

Информация, связанная с данной

[CHECKIN LIBVOLUME \(регистрация тома хранения в библиотеке\)](#)

[CHECKOUT LIBVOLUME \(исключение тома хранения из библиотеки\)](#)

Поддержание запаса чистых томов в автоматизированной библиотеке

Задавая пул хранения, связанный с автоматизированной библиотекой, вы можете указать максимальное число чистых томов, равное физической емкости библиотеки. Если сервер использует для пула хранения большее число чистых томов, вы должны убедиться, что у вас есть достаточное число доступных томов.

Процедура

Если число чистых томов, которые сервер использует для пула хранения, превысит максимальное число, заданное в определении пула хранения, выполните следующие шаги:

1. Добавьте в библиотеку чистые тома, введя команду **CHECKIN LIBVOLUME**.

Совет: Вам может потребоваться хранилище переполнения, чтобы можно было высвободить место для этих чистых томов путем перемещения томов из библиотеки. Дополнительную информацию смотрите в разделе [“Управление заполненной библиотекой с хранилищем переполнения”](#) на стр. 201.

2. Увеличьте максимальное число чистых томов, которые можно добавить в пул хранения, введя команду **UPDATE STGPOOL** и задав параметр **MAXSCRATCH**.

Дальнейшие действия

Вам может потребоваться больше томов для будущих операций восстановления, поэтому рассмотрите возможность снабдить метками и выделить несколько дополнительных чистых томов.

Задачи, связанные с данной

[Поддержание запаса чистых томов](#).

Вы должны задать для пула хранения достаточно большое максимальное число чистых томов в соответствии с ожидаемым уровнем использования.

Управление заполненной библиотекой с хранилищем переполнения

С ростом потребности в пространстве хранения число томов, необходимых в пуле хранения, может превысить физическую емкость автоматизированной библиотеки. Чтобы сделать пространство доступным для новых томов и чтобы отслеживать существующие тома, можно задать систему хранения переполнения для пула хранения.

Об этой задаче

Сервер отслеживает тома, перемещенные в зону переполнения, и делает слоты хранения доступными для новых томов.

Процедура

1. Создайте хранилище переполнения для томов. Задайте или обновите пул хранения, связанный с автоматизированной библиотекой, при помощи команды **DEFINE STGPOOL** или **UPDATE STGPOOL** с параметром **OVFLOCATION**.

Например, чтобы создать систему хранения переполнения с именем ROOM2948 для пула хранения с именем ARCHIVEPOOL, введите следующую команду:

```
update stgpool archivepool ovflocation=Room2948
```

2. Если вам нужно создать в библиотеке пространство для чистых томов, переместите заполненные тома в хранилище переполнения, введя команду **MOVE MEDIA**.
Например, чтобы переместить все заполненные тома в указанный пул хранения за пределами библиотеки, введите следующую команду:

```
move media * stgpool=archivepool
```

3. Активируйте новые чистые тома (если необходимо).

Ограничение: Если для тома есть запись в файле хронологии тома, то его нельзя зарегистрировать как чистый том. Дополнительную информацию смотрите в разделе [“Регистрация томов в автоматизированной библиотеке”](#) на стр. 191.

4. Определите пустые чистые ленты в хранилище переполнения, введя команду **QUERY MEDIA**.
Например, введите следующую команду:

```
query media * stg=* whereovflocation=Room2948 wherestatus=empty
```

5. Если сервер затребует дополнительные тома, найдите и активируйте тома из хранилища переполнения.

Чтобы найти тома в хранилище переполнения, введите команду **QUERY MEDIA**. Команду **QUERY MEDIA** также можно использовать для генерирования команд посредством активации томов.

Чтобы посмотреть список томов в хранилище переполнения и одновременно сгенерировать команды для активации этих томов в библиотеке, введите примерно следующую команду:

```
query media format=cmd stgpool=archivepool whereovflocation=Room2948  
cmd="checkin libvol autolib &vol status=private"  
cmdfilename="\storage\move\media\checkin.vols"
```

Советы:

- Требования монтирования от сервера содержат расположение томов.
- Чтобы задать срок в днях, по истечении которого тома станут подлежать обработке, введите команду **UPDATE STGPOOL** и задайте параметр **REUSEDELAY**.
- Файл, содержащий сгенерированную команду, можно запустить с помощью команды IBM Spectrum Protect **MACRO**.

Информация, связанная с данной

[MOVE MEDIA](#) (перемещение носителей пула хранения с последовательным доступом)

[QUERY MEDIA](#) (запрос о носителе пула хранения с последовательным доступом)

[UPDATE STGPOOL](#) (обновить пул хранения)

Аудит перечня томов в библиотеке

Можно выполнить аудит автоматизированной библиотеки, чтобы обеспечить соответствие инвентарного списка томов библиотеки и томов, которые физически в ней находятся. Можно выполнить аудит библиотеки в случае нарушения целостности перечня томов библиотеки из-за перемещения томов в библиотеке вручную или в связи с ошибками базы данных.

Процедура

1. Убедитесь, что на накопителях в библиотеке не смонтировано никаких томов. Если есть какие-либо смонтированные тома, которые находятся в состоянии IDLE, введите команду **DISMOUNT VOLUME**, чтобы их размонтировать.
2. Произведите аудит перечня томов, введя команду **AUDIT LIBRARY**. Выполните одно из следующих действий.
 - Если у библиотеки есть устройство чтения штрих-кодов, вы можете сэкономить время, воспользовавшись устройством чтения штрих-кодов для идентификации томов. Например, выполнить аудит библиотеки TAPELIB с помощью устройства считывания штрих-кода можно по следующей команде:

```
audit library tapelib checklabel=barcode
```
 - Если у библиотеки нет устройства для чтения штрих-кодов, введите команду **AUDIT LIBRARY**, не задавая параметр **CHECKLABEL=BARCODE**. Сервер монтирует каждый том, чтобы проверить метку. После проверки метки сервер завершит аудит всех остальных томов.

Результаты

Сервер удаляет из перечня отсутствующие тома и обновляет данные о расположении томов, перемещенных со времени последнего аудита.

Ограничение: Во время аудита сервер не может добавлять тома в перечень.

Задачи, связанные с данной

Запись меток томов на ленточных томах

Ленточные тома следует снабжать метками до их определения для сервера.

Информация, связанная с данной

AUDIT LIBRARY (аудит томов автоматизированной библиотеки)

DISMOUNT VOLUME (Размонтировать том, заданный по имени)

Частично записанные тома

Частично записанные тома всегда считаются закрытыми, даже если до их выбора сервером для монтирования они находились в состоянии чистых томов. Сервер отслеживает исходное состояние чистых томов и может вернуть им чистое состояние, когда они станут пустыми.

Кроме томов в автоматизированных библиотеках, сервер не располагает сведениями о чистом томе до его установки. Затем состояние тома меняется на закрытое, и том автоматически определяется как часть пула хранения, для которого был сделан запрос на монтирование.

Задачи, связанные с данной

Изменение состояния тома в автоматизированной библиотеке

Вы можете изменить состояние тома с `private` (закрытый) на `scratch` (чистый) или наоборот.

Операции с совместно используемыми библиотеками

Совместно используемые библиотеки - это логические библиотеки, представленные физически библиотеками SCSI. Физическая библиотека управляется сервером IBM Spectrum Protect, настроенным как менеджер библиотеки. Серверы IBM Spectrum Protect, на которых используется тип библиотек SHARED, являются клиентами библиотеки по отношению к серверу менеджера библиотеки IBM Spectrum Protect.

Клиент библиотеки связывается с диспетчером библиотек, когда запускается диспетчер библиотек и инициализируется устройство хранения, или после определения диспетчера библиотек клиенту библиотеки. Клиент библиотеки подтверждает, что сервер на связи является менеджером библиотеки для указанного библиотечного устройства. Клиент библиотеки также проверяет согласованность определений накопителей с менеджером библиотеки. Клиент

библиотеки связывается с менеджером библиотеки для выполнения каждой из следующих операций:

Монтирование тома

Клиент библиотеки посылает менеджеру библиотеки запрос на доступ к определенному тому совместно используемого библиотечного устройства. Для чистого тома клиент библиотеки имя не указывает. Если менеджеру библиотеки не удастся получить доступ к запрошенному тому, или если чистые тома недоступны, менеджер отклоняет запрос на монтирование. Если монтирование выполнено успешно, менеджер библиотеки возвращает имя накопителя, в который смонтирован том.

Освобождение тома

Если клиенту библиотеки больше не нужен доступ к тому, он сообщает менеджеру библиотеки, что том можно вернуть в чистое состояние. База данных менеджера библиотеки обновляется значением нового расположения для тома, который теперь находится в перечне библиотечного сервера. Том удаляется из перечня томов клиента библиотеки.

Таблица 35 на стр. 204 показывает взаимодействие между клиентами и менеджером библиотеки в процессе обработки операций IBM Spectrum Protect.

Таблица 35. Как серверы, поддерживающие SAN, обрабатывают операции IBM Spectrum Protect		
Операция (команда)	Менеджер библиотеки	Библиотечный клиент
Запрос томов библиотеки (QUERY LIBVOLUME)	Показывает тома, зарегистрированные в библиотеке. Для закрытых томов будет также показан сервер-владелец.	Неприменимо.
Регистрация и изъятие томов библиотеки (CHECKIN LIBVOLUME, CHECKOUT LIBVOLUME)	Посылает команды библиотечному устройству.	Неприменимо. Если операция активации должна быть выполнена из-за восстановления клиента, серверу менеджера библиотеки посылается требование.
Перемещение обычных носителей и носителей DRM (MOVE MEDIA, MOVE DRMEDIA)	Допустимо только для томов, используемых сервером менеджера библиотеки.	Запрашивает завершение операции сервером менеджера библиотеки. Вызывает процесс резервирования на сервере менеджера библиотеки.
Аудит перечня библиотеки (AUDIT LIBRARY)	Синхронизирует перечень с библиотечным устройством.	Синхронизирует перечень с сервером менеджера библиотеки.
Маркировка тома библиотеки (LABEL LIBVOLUME)	Помечает и активирует тома.	Неприменимо.
Размонтирование тома (DISMOUNT VOLUME)	Посылает запрос библиотечному устройству.	Запрашивает завершение операции сервером менеджера библиотеки.

Таблица 35. Как серверы, поддерживающие SAN, обрабатывают операции IBM Spectrum Protect (продолжение)

Операция (команда)	Менеджер библиотеки	Библиотечный клиент
Запрос тома (QUERY VOLUME)	Проверяет, владеет ли томом запрашиваемый клиент библиотеки и находится ли этот том в библиотечном устройстве.	Запрашивает завершение операции сервером менеджера библиотеки.

Управление серверными запросами на тома

IBM Spectrum Protect показывает требования и сообщения о состоянии во всех клиентах командой строки администрирования, запущенных в режиме консоли. Часто эти запросы ограничены по времени. Успешные операции сервера должны быть выполнены в рамках заданного предела времени; в противном случае произойдет тайм-аут операции.

Об этой задаче

Для автоматизированных библиотек используйте команды **CHECKIN LIBVOLUME** и **LABEL LIBVOLUME**, чтобы вставить картриджи в слоты. Если вы зададите значение параметра **WAITTIME**, то появится ответное сообщение. Если значение параметра равно нулю, ответ не требуется. Введя команду **CHECKOUT LIBVOLUME**, вы должны будете вставить картриджи в слоты, и во всех случаях появится ответное сообщение.

Процедура

- В следующей таблице представлена информация, как обрабатывать различные задачи для носителей сервера.

Задача	Подробности
Использование клиента администрирования при работе с запросами на монтирование	Сервер отправляет сообщения о состоянии запросов на монтирование на серверную консоль и всем клиентам командной строки администрирования, которые были запущены в режиме монтирования или режиме консоли Для запуска клиента командной строки администрирования в режиме монтирования введите команду dsmdmc -mountmode в клиенте командной строки администрирования.
Получение сообщений об автоматизированных библиотеках	Сообщения монтирования и сообщения об ошибках можно просматривать в автоматизированных библиотеках на клиентах командной строки администрирования в режиме монтирования или в режиме консоли. Сообщения монтирования посылаются в библиотеку, а не оператору. Сообщения о неполадках библиотеки отсылаются в очередь сообщений, связанных с монтированием.
Получение сведений о запросах к оператору, ожидающих выполнения	Для получения информации об отложенных требованиях для оператора введите команду QUERY REQUEST или просмотрите очередь сообщений монтирования на клиенте командной строки администрирования, запущенном в режиме монтирования. При использовании команды QUERY REQUEST сервер показывает запрашиваемые действия и время, оставшееся до истечения ожидания запрашиваемых действий.

Задача	Подробности
<p>Ответ на запросы к оператору</p>	<p>Когда сервер требует явного ответа на выполненный запрос монтирования, используйте команду REPLY.</p> <p>Параметр <i>номер_требования</i> задает идентификационный номер требования, указывающий серверу, какое из отложенных требований оператора выполнено. Этот трехзначный номер всегда появляется в сообщении с запросом.</p>
<p>Отмена требования для оператора</p>	<p>Чтобы отменить требование монтирования для библиотеки, введите команду CANCEL REQUEST. Для большинства запросов, связанных с автоматизированными библиотеками SCSI, оператор должен выполнить программное или аппаратное действие, чтобы отменить запрошенное монтирование. В случаях с такими запросами сервер не допускает использование команды CANCEL REQUEST.</p> <p>Команда CANCEL REQUEST должна содержать идентификационный номер запроса. Это номер указан в тексте запроса.</p> <p>Чтобы пометить запрашиваемый том как UNAVAILABLE, введите команду CANCEL REQUEST, задав параметр PERMANENT. Если задать параметр PERMANENT, то сервер не будет снова пытаться смонтировать запрошенный том. Например, это полезно, если том находится на удаленной площадке или недоступен по другой причине.</p>
<p>Ответ на требование активации тома</p>	<p>Если серверу не удастся обнаружить в автоматизированной библиотеке определенный том, который должен быть смонтирован, оператор получит запрос на регистрацию этого тома.</p> <p>Если запрашиваемый том доступен, поместите его в библиотеку и активируйте. Дополнительную информацию смотрите в разделе “Регистрация томов в автоматизированной библиотеке” на стр. 191.</p> <p>Если затребованный том недоступен, измените режим доступа к тому, введя команду UPDATE VOLUME и задав параметр ACCESS=UNAVAILABLE. Затем отмените требование активации с помощью команды CANCEL REQUEST. Не отменяйте клиентский процесс, в результате которого был создан данный запрос. Используйте команду QUERY REQUEST для получения ID запроса, который вы хотите отменить.</p> <p>Если запрос сервера об активации тома не будет выполнен в течение периода ожидания монтирования для данного класса устройств в пуле хранения, то сервер пометит данный том как недоступный.</p>
<p>Как определить, какие тома смонтированы</p>	<p>Чтобы получить отчет о всех томах, которые в настоящий момент смонтированы для использования сервером, введите команду QUERY MOUNT. Этот отчет содержит сведения о том, какие тома смонтированы, какие накопители обращались к ним и какие тома используются.</p>
<p>Размонтирование бездействующих томов</p>	<p>Если том бездействует, то сервер оставляет его смонтированным в течение времени, заданного параметром задержки размонтирования для данного класса устройств. Использование задержки размонтирования позволяет сократить время доступа, если тома используются повторно.</p> <p>Чтобы размонтировать бездействующий том с диска, на котором он смонтирован, введите команду DISMOUNT VOLUME.</p> <p>Дополнительные сведения о настройке времени задержки размонтирования смотрите в разделе “Управление интервалом времени, в течение которого том остается смонтированным” на стр. 134.</p>

Информация, связанная с данной

[QUERY REQUEST](#) (Запросить информацию об одном или нескольких отложенных требованиях монтирования)

Управление ленточными накопителями

Вы можете запрашивать информацию о ленточных накопителях, обновлять их или удалять. Можно также очищать ленточные устройства и конфигурировать шифрование ленточного устройства и проверку правильности данных.

Обновление накопителей

Вы можете изменить атрибуты определения накопителя, чтобы перевести накопитель в отключенное состояние или деконфигурировать его.

Об этой задаче

Можно изменить следующие атрибуты накопителя:

- Адрес элемента, если накопитель находится в SCSI
- Частота очистки
- Состояние накопителя: подключен или отключен

Ограничение: Если накопитель используется, вы не можете изменить ни номер элемента, ни имя устройства. Инструкции по отключению накопителей смотрите в разделе [“Отключение ленточных накопителей”](#) на стр. 208.

Если том смонтирован в накопителе, но он бездействует, его можно размонтировать явным образом. Инструкции по размонтированию бездействующего тома смотрите в разделе [“Управление серверными запросами на тома”](#) на стр. 205.

Процедура

- Измените адрес элемента накопителя, введя команду **UPDATE DRIVE**. Например, измените в библиотеке AUTO адрес элемента DRIVE3 на 119, введя следующую команду:

```
update drive auto drive3 element=119
```

- Измените имя устройства для накопителя, введя команду **UPDATE PATH**. Например, чтобы изменить имя устройства накопителя с именем DRIVE3, введите следующую команду:

```
AIX update path server1 drive3 srctype=server desttype=drive library=scsilib  
device=/dev/rmt0
```

```
Linux update path server1 drive3 srctype=server desttype=drive library=scsilib  
device=/dev/IBMtape0
```

```
Windows update path server1 drive3 srctype=server desttype=drive library=scsilib  
device=mt3.0.0.0
```

Информация, связанная с данной

[UPDATE DRIVE](#) (обновление накопителя)

[UPDATE PATH](#) (изменение пути)

Отключение ленточных накопителей

Ленточный накопитель можно отключить в процессе его использования. Например, можно отключить накопитель для обслуживания.

Об этой задаче

Если вы измените состояние накопителя на отключенное, когда накопитель используется, сервер завершит обработку ленты, находящейся в накопителе, а затем прекратит использовать накопитель. Однако если лента, которая использовалась, была частью серии лент для одной транзакции, накопитель не сможет завершить эту серию. Если других доступных накопителей нет, то операция может быть неудачной.

Процедура

- Чтобы изменить состояние накопителя, введите команду **UPDATE DRIVE** и задайте параметр **ONLINE**. Например, чтобы обновить накопитель DRIVE3 в библиотеке MANLIB и перевести диск в отключенное состояние, введите следующую команду:

```
update drive manlib drive3 online=no
```

Ограничение: Вместе с параметром **ONLINE** не следует указывать другие необязательные параметры. При этом накопитель не будет обновлен, а команда не будет выполнена, если накопитель используется.

Результаты

Если вы обновите в библиотеке все диски, переведя их в отключенное состояние, процессы, которым требуется точка монтирования библиотеки, завершатся неудачно.

Обновленное состояние накопителя сохраняется даже в случае остановки и перезапуска сервера. Если накопитель помечен как отключенный при перезапуске сервера, появляется предупреждение, сообщающее, что накопитель следует подключить вручную.

Информация, связанная с данной

[UPDATE DRIVE \(обновление накопителя\)](#)

Проверка данных при операциях записи на ленту или чтения с ленты

Для проверки данных и выявления поврежденных данных можно использовать функцию под названием 'защита логических блоков'. При использовании защиты логических блоков IBM Spectrum Protect вставляет значение проверки контрольной суммы в конце каждого логического блока данных, который записывается на ленту.

С помощью защиты логических блоков можно обнаруживать ошибки, происходящие при записи данных на ленту и при передаче данных с ленточного устройства в IBM Spectrum Protect через сеть хранения данных. Устройства, поддерживающие защиту логических блоков, проверяют данные во время операций чтения и записи. Сервер IBM Spectrum Protect проверяет данные во время операций чтения.

Если проверка на устройстве завершается с ошибкой во время операций записи, это может означать, что данные повреждены при передаче на ленту. В таком случае сервер IBM Spectrum Protect завершает операцию записи с ошибкой. Необходимо перезапустить операцию, чтобы продолжить работу. Если проверка на устройстве выдает ошибку во время операции чтения, это может означать, что ленточный носитель поврежден. Если проверка на сервере IBM Spectrum Protect выдает ошибку во время операции чтения, это может означать, что данные повреждены при передаче с ленточного устройства; сервер попытается выполнить операцию еще раз. Если проверка постоянно завершается с ошибкой, сервер IBM Spectrum Protect создает сообщение об ошибке, которое означает проблему оборудования или подключения.

Если защита логических блоков отключена на ленточном устройстве или это устройство не поддерживает защиту логических блоков, сервер IBM Spectrum Protect может прочитать защищенные данные. Однако эти данные не проверяются.

Защита логических данных лучше защиты контрольной суммы, которую можно задать при определении или обновлении пула хранения. Если вы зададите проверку CRC для пула хранения, то данные будут проверяться только в ходе операций по аудиту томов. Ошибки выявляются после записи данных на ленту.

ограничения:

- Нельзя использовать защиту логических блоков для последовательных данных, таких как наборы резервных копий и резервные копии базы данных.
- Проверка CRC отрицательно влияет на производительность, так как и на клиенте, и на сервере для вычисления и сравнения значений CRC потребуется использовать больше процессорных ресурсов.
- В случае чистого тома, если вы зададите защиту логического блока для операций чтения-записи (**LBPROTECT=READWRITE**), никогда не изменяйте значение параметра после записи данных на том. Изменение значения параметра в течение срока жизни тома на сервере IBM Spectrum Protect не поддерживается.

Накопители, поддерживающие защиту логических блоков

Защита логических блоков доступна только для устройств типов 3592, LTO и ECARTRIDGE. В число поддерживаемых накопителей 3592 входят IBM TS1130, TS1140 и последующие поколения. К возможным накопителям LTO относятся накопители LTO-5 и поддерживаемые накопители LTO-6. В число поддерживаемых накопителей Oracle StorageTek входят накопители с форматом T10000C и T10000D.

В следующей таблице показаны носители и форматы, которые можно использовать с накопителями, поддерживающими защиту логических блоков.

Накопитель	Ленточный носитель	Форматы накопителей
IBM TS1130	3592 Generation 2	3592-3 и 3592-3C
IBM TS1140	3592 Generation 2 3592 поколения 3	Поколение 2: 3592-3 и 3592-3C Поколение 3: 3592-4 и 3592-4C
IBM TS1150	3592 поколения 3 3592, поколение 4	Поколение 4: 3592-5 и 3592-5C
IBM LTO-5	LTO-5	Ultrium 5 и Ultrium 5C
IBM LTO-6	LTO-6 LTO-5	Ultrium 6 и Ultrium 6C Ultrium 5 и Ultrium 5C
IBM LTO-7	LTO-7 LTO-6	Ultrium 7 и Ultrium 7C Ultrium 6 и Ultrium 6C
Oracle T10000C	Oracle StorageTek T10000 T2	T10000C и T10000C-C
Oracle T10000D	Oracle StorageTek T10000 T2	T10000D и T10000D-C

Советы:

- Чтобы включить логическую защиту блока для ленточного тома и затем снова использовать том для поддержки данных, надо включить логическую защиту блока для класса устройства и диска.

- Если у вас есть накопитель 3592, LTO или Oracle StorageTek, не поддерживающий защиту логических блоков, его программно-аппаратное обеспечение можно обновить до версии, поддерживающей защиту логических блоков.

Доступна защита логических блоков для накопителей в библиотеках SCSI . Самую свежую информацию о поддержке защиты логических блоков смотрите в [техническом замечании 1568108](#).

Чтобы можно было использовать защиту логических блоков для операций записи, все накопители в библиотеке должны поддерживать защиту логических блоков. Если накопитель не поддерживает защиту логических блоков, тома, доступные для чтения и записи, монтироваться не будут. Однако сервер может использовать такой накопитель для монтирования томов, доступных только для чтения. Защищенные данные читаются и проверяются сервером IBM Spectrum Protect, если включена поддержка защиты логических блоков для операций чтения/записи.

Включение и отключение защиты логических блоков

Вы можете определить защиту логических блоков для операций чтения и записи или только для операций записи. Также можно выключить защиту логических блоков. По умолчанию защита логических блоков отключена, так как проверка контрольной суммы (cyclic redundancy check, CRC) на сервере и на ленточном устройстве влияет на производительность.

Об этой задаче

Операции чтения/записи для освобождения или заполнения томов зависят от наличия в томе защиты логических блоков. Защищенные и незащищенные блоки нельзя смешивать в одном томе. Если изменить параметр защиты логических блоков, это изменение будет применено только к пустым томам. Заполняемые и полные тома поддерживают свое состояние защиты логических блоков, пока они не будут пустыми и готовыми для нового заполнения. Например, если сервер выберет том, связанный с классом устройств с защитой логических блоков, сервер продолжит запись защищенных данных на этот том.

Ограничение: Защита логических блоков доступна только для некоторых типов устройств. Дополнительную информацию смотрите в разделе [“Накопители, поддерживающие защиту логических блоков”](#) на стр. 209.

Процедура

1. Чтобы включить защиту логических блоков для типов устройств 3592, LTO и ECARTRIDGE, введите команду **DEFINE DEVCLASS** или **UPDATE DEVCLASS** и задайте параметр **LBPROTECT**. Например, чтобы задать защиту логических блоков во время операций чтения и записи для класса устройств 3592 с именем 3592_lbprotect, введите следующую команду:

```
define devclass 3592_lbprotect library=3594 lbprotect=readwrite
```

Советы:

- Если изменить значение параметра **LBPROTECT** с NO на READWRITE или WRITEONLY и сервер выберет заполняющийся том без защиты логических блоков, он будет выдавать сообщение при всяком монтировании тома. Это сообщение информирует, что данные будут записаны в том без защиты логических блоков. Чтобы предотвратить появление этого сообщения или чтобы IBM Spectrum Protect выполнял запись данных только с защитой логических блоков, сделайте заполняющиеся тома без защиты логических блоков доступными только для чтения.
- Чтобы повысить производительность, не указывайте параметр **CRCDATA** в команде **DEFINE STGPPOOL** или **UPDATE STGPPOOL**.
- Когда данные проверяются во время операций чтения как на накопителе, так и на сервере IBM Spectrum Protect, это может привести к снижению производительности сервера во время операций восстановления и извлечения. Чтобы сократить время, которое требуется для выполнения операций по восстановлению и извлечению данных, измените значение параметра **LBPROTECT** с READWRITE на WRITEONLY. После восстановления или извлечения данных можно снова изменить значение параметра **LBPROTECT** на READWRITE.

2. Чтобы выключить защиту логических блоков, введите команду **DEFINE DEVCLASS** или **UPDATE DEVCLASS** и задайте параметр **LBPROTECT=NO**.

Ограничение: Если защита логических блоков отключена, сервер не выполняет запись на пустую ленту с защитой логических блоков. Однако если выбран заполняющийся том с защитой логических блоков, сервер продолжит запись в том с защитой логических блоков. Чтобы сервер не выполнял запись на ленту с защитой логических блоков, сделайте заполняющиеся тома с защитой логических блоков доступными только для чтения. При чтении данных результаты CRC (контрольной суммы) не проверяются ни на накопителе, ни на сервере.

Если произойдет авария и на площадке восстановления после аварии не окажется накопителей, поддерживающих защиту логических блоков, нужно задать параметр **LBPROTECT=NO**. Если для записи используются ленточные накопители, то нужно заменить доступ к томам с защищенными данными на "только для чтения", чтобы сервер не использовал эти тома.

Если сервер должен включить защиту логических блоков, сервер выдает сообщение об ошибке, которое указывает, что накопитель не поддерживает защиту логических блоков.

Дальнейшие действия

Для определения, есть ли у тома защита логических блоков, введите команду **QUERY VOLUME** и проверьте значение в поле Защита логических блоков.

Информация, связанная с данной

[DEFINE DEVCLASS \(Задать класс устройств\)](#)

[DEFINE STGPOOL \(определение тома в пуле хранения\)](#)

[QUERY VOLUME \(Запросить информацию о томах пула хранения\)](#)

[UPDATE DEVCLASS \(изменение класса устройства\)](#)

[UPDATE STGPOOL \(обновить пул хранения\)](#)

Операции чтения/записи для томов с защитой логических блоков

Операции чтения/записи для освобождения или заполнения томов зависят от наличия в томе защиты логических блоков. Защищенные и незащищенные блоки нельзя смешивать в одном томе.

Если для изменения параметра защиты логических блоков используется команда **UPDATE DEVCLASS**, это изменение применяется только к пустым томам. Заполняемые и полные тома поддерживают свое состояние защиты логических блоков, пока они не будут пустыми и готовыми для нового заполнения.

Предположим, например, что вы измените значение параметра **LBPROTECT** с READWRITE на NO. Если сервер выберет том, который связан с классом устройства и на котором задана защита логических блоков, сервер по-прежнему будет записывать на том защищенные данные.

Советы:

- Если накопитель не поддерживает защиту логических блоков, смонтировать тома с защитой логических блоков для операций записи не удастся. Чтобы предотвратить монтирование сервером защищенных томов для операций записи, измените доступ к тому на предназначенный только для чтения. Отключите также защиту логических блоков, чтобы предотвратить включение сервером этой возможности для ленточных накопителей.
- Если диск не поддерживает защиту логических блоков и такая защита отключена, сервер читает данные с защищенных томов. Однако эти данные не проверяются сервером и ленточным накопителем.

Информация, связанная с данной

[QUERY VOLUME \(Запросить информацию о томах пула хранения\)](#)

[UPDATE DEVCLASS \(изменение класса устройства\)](#)

Управление пулами хранения в ленточной библиотеке

Чтобы хранить в одной библиотеке и защищенные, и незащищенные данные, надо создать различные классы устройств и различные пулы хранения для разделения этих данных. Если класс устройства связан с защищенными данными, вы можете определить защиту логических блоков для операций чтения и записи или только для операций записи.

Чтобы задать классы устройства и пулы хранения для библиотеки TS3500 с накопителями LTO-5 для защищенных и незащищенных данных, можно ввести ряд команд, как показано в следующем примере:

```
define library 3584 libtype=scsi
define devclass lbprotect library=3584 devicetype=lto lbprotect=readwrite
define devclass normal library=3584 devicetype=lto lbprotect=no
define stgpool lbprotect_pool lbprotect maxscratch=10
define stgpool normal_pool normal maxscratch=10
```

Информация, связанная с данной

[DEFINE DEVCLASS \(Задать класс устройств\)](#)

[DEFINE LIBRARY \(Задать библиотеку\)](#)

[DEFINE STGPOOL \(определение тома в пуле хранения\)](#)

Очистка ленточных накопителей

Сервер можно использовать для управления очисткой ленточных накопителей. Сервер может управлять тем, как производится очистка ленточных накопителей в библиотеках SCSI.

Об этой задаче

Для очистки ленточных накопителей необходимы системные полномочия или неограниченные полномочия на хранение. В случае автоматизированных библиотек можно автоматизировать очистку, задав частоту операций очистки и зарегистрировав чистящий картридж в перечне томов библиотеки. IBM Spectrum Protect смонтирует чистящий картридж в соответствии с заданными значениями. Особые замечания касаются случая, когда планируется использовать очистку накопителей под управлением сервера в библиотеке SCSI, которая поддерживает автоматическую очистку накопителей на аппаратном уровне.

Совет: Если автоматизированная ленточная библиотека поддерживает очистку накопителей в библиотеке, убедитесь, что эта функция включена.

Вы можете предотвратить преждевременное изнашивание головок для чтения и записи накопителей, используя функции очистки библиотеки, которые предоставляет ваш производитель устройств.

Накопители и библиотеки от разных производителей различаются тем, как они управляют чистящими картриджами и как они сообщают о присутствии чистящего картриджа в накопителе. Драйвер устройства может не открыть накопитель, в котором содержится чистящий картридж. Коды считывания и коды ошибок, выдаваемые устройствами для чистки накопителя, отличаются. Очистка накопителей библиотеки обычно неизвестна приложениям. В связи с этим IBM Spectrum Protect не всегда обнаруживает чистящие картриджи в накопителях и может не определить время начала чистки.

Некоторые устройства требуют небольшой период простоя между запросами на монтирование для запуска чистки накопителя. Однако IBM Spectrum Protect пытается свести к минимуму время простоя накопителя. Результатом может быть неэффективное выполнение чистки накопителя библиотеки. Если это происходит, используйте IBM Spectrum Protect для управления очисткой накопителей. Можно задать частоту очистки в соответствии с рекомендациями производителя.

Методы очистки ленточных накопителей

Со временем читающие головки ленточных накопителей могут загрязниться, что может вызвать ошибки чтения и записи. Чтобы предотвратить эти проблемы, включите очистку магнитных лент. Очистку лент можно включить с накопителя или из IBM Spectrum Protect.

Можно выбрать использование способа очистки библиотечного накопителя или способ очистки накопителя IBM Spectrum Protect, но не оба способа одновременно. Некоторые библиотеки SCSI обеспечивают возможность автоматической очистки накопителей. Выберите метод очистки библиотечных накопителей, если он доступен. Если он недоступен или вызывает проблемы, используйте IBM Spectrum Protect для управления очисткой библиотечных накопителей.

Метод очистки библиотечных накопителей

У способа очистки библиотечных накопителей есть несколько преимуществ для автоматических ленточных библиотек, использующих эту функцию:

- Понижается нагрузка на администратора IBM Spectrum Protect по физическому управлению очисткой картриджей.
- Снижается интенсивность использования картриджей очистки. Большинство библиотек отслеживает, сколько раз можно очищать ленты, на основании индикаторов аппаратных компонентов. IBM Spectrum Protect использует необработанное число.
- Уменьшает число необязательных очисток. В современных ленточных носителях не требуются очистки через фиксированные интервалы времени, так как они могут определить, когда нужна очистка, и затребовать ее.

Производители, которые предоставляют метод очистки библиотечных накопителей, рекомендуют его использовать, чтобы предотвратить преждевременный износ головок чтения/записи в накопителях. Накопители и библиотеки от разных производителей различаются тем, как они управляют чистящими картриджами и как они сообщают о присутствии чистящего картриджа в накопителе. Драйвер устройства может не открыть накопитель, в котором содержится чистящий картридж. Коды считывания и коды ошибок, выдаваемые устройствами для чистки накопителя, отличаются. Чистка накопителя библиотеки обычно скрыта от программ. Однако IBM Spectrum Protect не всегда обнаруживает чистящие картриджи в накопителях и может не определить время начала чистки.

Способы очистки накопителей IBM Spectrum Protect

Некоторые устройства требуют небольшой период простоя между запросами на монтирование для запуска чистки накопителя. Однако IBM Spectrum Protect пытается свести к минимуму время простоя накопителя. Результатом может быть неэффективное выполнение чистки накопителя библиотеки. Если это происходит, попробуйте использовать IBM Spectrum Protect для управления чисткой накопителей. Установите частоту очистки, соответствующую рекомендациям производителя.

Если IBM Spectrum Protect управляет процессом очистки накопителей, отключите функцию очистки библиотечных накопителей, чтобы избежать проблем. Если включена функция очистки библиотечных носителей, некоторые устройства автоматически перемещают чистящий картридж, обнаруженный в библиотеке, в выделенные для него слоты библиотеки. Невозможно зарегистрировать чистящий картридж в перечне библиотеки IBM Spectrum Protect, пока не отключена собственная функция очистки библиотечных носителей.

Чтобы включить очистку с накопителя, следуйте инструкциям, которые предоставляет производитель накопителя. Чтобы узнать, как включить очистку с использованием IBM Spectrum Protect, смотрите раздел [“Конфигурирование сервера для очистки накопителей в автоматизированной библиотеке”](#) на стр. 213.

Конфигурирование сервера для очистки накопителей в автоматизированной библиотеке

При конфигурировании очистки накопителей в автоматизированной библиотеке под управлением сервера вы можете указать, как часто должна производиться чистка накопителей.

Прежде чем начать

Определите, как часто следует производить очистку накопителя. Этот шаг необходим, чтобы вы смогли задать соответствующее значение для параметра **CLEANFREQUENCY** в команде **DEFINE DRIVE** или **UPDATE DRIVE**. Например, чтобы производить очистку накопителя после обработки 100 ГБ данных на накопителе, задайте параметр **CLEANFREQUENCY=100**.

Рекомендации по частоте очистки смотрите в документации производителя накопителей. Если в документации представлены рекомендации по частоте очистки, исходя из часов использования, преобразуйте значение в гигабайты, выполнив следующие шаги:

1. На основе значения 'байт в секунду' для накопителя определите значение в гигабайтах в час.
2. Умножьте значение в гигабайтах в час на рекомендуемое количество часов использования между чистками.
3. Результатом этого действия и будет частота очистки.

Можно задать либо значение параметра **CLEANFREQUENCY**, либо можно указать **ASNEEDED**, чтобы производить очистку накопителя, когда это потребуется.

ограничения:

1. Для накопителей IBM 3592 нужно задавать числовое значение параметра **CLEANFREQUENCY**. Если использовать частоту очистки, указанную в документации по продукту, вы не произведете очистку накопителей сверх необходимого.
2. Значение параметра **CLEANFREQUENCY=ASNEEDED** работает не для всех ленточных накопителей. Чтобы узнать, поддерживает ли накопитель данную функцию, смотрите информацию для вашей операционной системы:

AIX	Windows	Поддерживаемые устройства для AIX и Windows
Linux		Поддерживаемые устройства для Linux

В техническом замечании щелкните по имени накопителя, чтобы увидеть подробную информацию. Если значение ASNEEDED не поддерживается, задайте число гигабайт.

Процедура

Определите или измените накопители в библиотеке, используя параметр **CLEANFREQUENCY** в командах **DEFINE DRIVE** или **UPDATE DRIVE**.

Например, чтобы производить очистку накопителя DRIVE1 после обработки 100 ГБ данных, введите следующую команду:

```
update drive autolib1 drive1 cleanfrequency=100
```

Результаты

После того как чистящий картридж будет зарегистрирован, сервер будет монтировать его в накопитель, когда понадобится произвести очистку. Сервер будет использовать чистящий картридж для указанного числа очисток. Дополнительную информацию смотрите в разделе [“Операции с чистящими картриджами”](#) на стр. 163.

Дальнейшие действия

Активируйте чистящий картридж в перечне томов библиотеки, следуя инструкциям в разделе [“Активация чистящего картриджа в библиотеке”](#) на стр. 214.

Информация, связанная с данной

[DEFINE DRIVE \(Задать накопитель для библиотеки\)](#)

[UPDATE DRIVE \(обновление накопителя\)](#)

Активация чистящего картриджа в библиотеке

Чтобы включить автоматическую очистку ленточных накопителей, нужно активировать чистящий картридж в перечне томов автоматизированной библиотеки.

Об этой задаче

При активации чистящего картриджа в библиотеке убедитесь, что он правильно идентифицирован сервером как чистящий картридж. Убедитесь, что чистящий картридж не находится в слоте, который обнаружен процессом поиска. Из-за неправильно расположенного чистящего картриджа могут возникать ошибки и задержки до 15 минут и более.

Предпочтительный метод заключается в активации чистящих картриджей по отдельности. Если вам нужно активировать как картриджи с данными, так и чистящие картриджи, сначала поместите картриджи с данными в библиотеку и активируйте их. Затем отдельно активируйте чистящий картридж в библиотеке.

Процедура

Чтобы активировать чистящий картридж в библиотеке, введите команду **CHECKIN LIBVOLUME**. Например, чтобы активировать чистящий картридж с именем AUTOLIB1, введите следующую команду:

```
checkin libvolume autolib1 cleanv status=cleaner cleanings=10  
checklabel=no
```

Сервер попросит поместить картридж в порт входа/выхода или в конкретный слот.

Информация, связанная с данной

[CHECKIN LIBVOLUME \(регистрация тома хранения в библиотеке\)](#)

Операции с чистящими картриджами

Чтобы убедиться, что ленточные накопители подвергаются очистке, когда это необходимо, и чтобы избежать проблем с пространством хранения на ленте, следуйте рекомендациям.

Мониторинг процесса очистки

Если в библиотеке активируется чистящий картридж и нужно очистить накопитель, сервер размонтирует том данных и запустит операцию очистки. Если операция очистки завершится неудачно или будет отменена либо если чистящего картриджа нет, вы можете не узнать, что требуется очистка накопителя. Из-за этой проблемы необходимо следить за сообщениями об очистке, чтобы обеспечить своевременную очистку накопителей. При необходимости введите команду **CLEAN DRIVE**, чтобы сервер попытался еще раз произвести очистку, или вручную загрузите чистящий картридж в накопитель.

Использование нескольких чистящих картриджей

Сервер будет использовать чистящий картридж для числа очисток, указанного при регистрации чистящего картриджа. Если зарегистрировать два или несколько чистящих картриджей, сервер будет использовать только один из них, пока не будет достигнуто заданное для картриджа число очисток. Затем сервер использует следующий чистящий картридж. Если зарегистрировать два или несколько чистящих картриджей и ввести две или несколько команд **CLEAN DRIVE** одновременно, сервер будет использовать несколько картриджей одновременно и зарегистрирует оставшееся количество очисток для каждого картриджа.

Информация, связанная с данной

[AUDIT LIBRARY \(аудит томов автоматизированной библиотеки\)](#)

[CHECKIN LIBVOLUME \(регистрация тома хранения в библиотеке\)](#)

[CLEAN DRIVE \(очистка накопителя\)](#)

[LABEL LIBVOLUME \(запись метки на том библиотеки\)](#)

[QUERY LIBVOLUME \(Запросить информацию о томе библиотеки\)](#)

Устранение ошибок, связанных с очисткой накопителей

При перемещении картриджей в библиотеке вы можете поместить картридж с данными туда, где должен находиться чистящий картридж. Ознакомьтесь с процессом, который выполнит сервер, и генерируемыми сообщениями, чтобы вы смогли устранить проблему.

Когда требуется очистить накопитель, сервер загружает в него картридж, который, согласно его базе данных, должен быть чистящим. Затем накопитель переходит в состояние READY и IBM Spectrum Protect определяет, что картридж является картриджем данных. Сервер выполняет следующие действия:

1. Сервер пытается считать внутреннюю метку ленты из картриджа данных.

2. Сервер извлекает картридж из накопителя и перемещает его в обратном направлении в слот для чистящего картриджа в пределах библиотеки. Если извлечение не удастся, то сервер помечает накопитель как отключенный и выдает сообщение, что картридж все еще находится в накопителе.
3. Сервер резервирует чистящий картридж, чтобы предотвратить его повторный выбор для следующего запроса очистки накопителя. Чистящий картридж остается в библиотеке, но больше не фигурирует в перечне библиотеки IBM Spectrum Protect.
4. Сервер сравнивает имя тома с текущим перечнем библиотеки, томами пула хранения и файлом хронологии томов, используя внутреннюю метку ленты.
 - Если имя тома не найдено в перечне библиотеки, возможно, картридж с данными был по ошибке активирован как чистящий картридж. При отмене активации тома никаких дальнейших действий от вас не требуется.
 - Если имя тома найдено в перечне библиотеки, сервер сгенерирует сообщение о том, что требуется вмешательство оператора и аудит библиотеки. Чтобы устранить проблему, выполните инструкции из раздела [“Аудит перечня томов в библиотеке”](#) на стр. 202.

Замена ленточного накопителя

Если заменяется накопитель в ленточной библиотеке, определенной для IBM Spectrum Protect, то необходимо удалить описание старого накопителя и пути к нему, а затем определить новый накопитель и путь.

Замена определений накопителей и путей необходима, даже если используется новый накопитель того же типа, тот же логический адрес, физический адрес, идентификатор SCSI и номер порта. Алиасы устройств могут меняться при изменении подключений накопителей.

Если новый накопитель поддерживает новый формат носителей, то может возникнуть необходимость описать новую логическую библиотеку, класс устройства и пул хранения. Процедуры настройки политики для нового накопителя в библиотеке с несколькими накопителями зависят от типов накопителей и носителей в библиотеке.

Удаление ленточных накопителей

Из библиотеки можно удалять ленточные накопители. Например, можно удалить накопитель, который вы больше не используете, или накопитель, который вы хотите заменить.

Процедура

1. Завершите работу сервера IBM Spectrum Protect и операционной системы.
2. Удалите старый накопитель и, следуя инструкциям производителя, установите новый накопитель.
3. Перезапустите операционную систему и сервер IBM Spectrum Protect.
4. Удалите путь от сервера к накопителю.

Например, чтобы удалить путь от SERVER1 до LIB1, введите следующую команду:

```
delete path server1 lib1 srctype=server desttype=drive
```

5. Удалите описание накопителя.
Например, введите следующую команду, чтобы удалить накопитель с именем DLT1 из библиотечного устройства с именем LIB1:

```
delete drive lib1 dlt1
```

Информация, связанная с данной

[DELETE DRIVE \(Удалить накопители из библиотеки\)](#)

[DELETE PATH \(удаление пути\)](#)

Замена накопителей другими накопителями того же типа

Чтобы добавить накопитель, поддерживающий тот же формат носителей, что и заменяемый им накопитель, нужно задать новое устройство и путь.

Об этой задаче

Если в библиотеке есть только одна модель накопителя и вы хотите заменить накопитель, вы должны заменить накопитель накопителем той же модели. Если в библиотеке есть комбинация моделей накопителей и вы хотите заменить накопитель, вы должны заменить накопитель накопителем любой модели, которая существует в библиотеке.

Процедура

1. Удалите определения пути и накопителя для старого накопителя. Например, чтобы удалить накопитель с именем DRIVE1 из библиотеки LIB1, введите следующую команду:

```
delete path server2 drive1 srctype=server desttype=drive library=lib1
delete drive lib1 drive1
```

2. Выключите библиотеку, размонтируйте исходный накопитель, замените его новым накопителем и включите библиотеку.
3. Обновите хост-систему, чтобы убедиться, что система обнаружила новый накопитель.
4. Опишите новый накопитель и путь. Например, чтобы задать новый накопитель, DRIVE2, и путь к нему с сервера SERVER2, если вы используете драйвер устройств IBM Spectrum Protect, введите следующие команды:

```
AIX define drive lib1 drive2
define path server2 drive2 srctype=server desttype=drive library=lib1
device=/dev/mt0
```

```
Linux define drive lib1 drive2
define path server2 drive2 srctype=server desttype=drive library=lib1
device=/dev/tmscsi/mt0
```

```
Windows define drive lib1 drive2
define path server2 drive2 srctype=server desttype=drive library=lib1
device=mt3.0.0.1
```

Совет: Можно использовать существующие описания библиотек, классов устройства и пулов хранения.

Информация, связанная с данной

[DELETE DRIVE \(Удалить накопители из библиотеки\)](#)

[DELETE PATH \(удаление пути\)](#)

Перенос данных на обновленные накопители

Если вы обновляете все ленточные накопители в библиотеке, вы можете сохранить существующие определения правил политики, чтобы производить перенос и удаление устаревших существующих данных, и сможете использовать новые накопители для сохранения данных.

Прежде чем начать

В следующем сценарии предполагается, что у вас уже есть первичный пул хранения для класса устройств DISK с именем POOL1.

Процедура

1. Чтобы перенести данные в пул хранения, созданный для новых накопителей, задайте параметр **NEXTSTGPOOL**. Например, чтобы перенести данные из существующего пула хранения POOL1 в новый пул хранения, POOL2, введите следующую команду:

```
update stgpool pool1 nextstgpool=pool2
```

2. Измените определения классов управления, чтобы сохранить данные в новом пуле хранения DISK, при помощи команды **UPDATE MGMTCLASS**.

Информация, связанная с данной

[DEFINE STGPOOL](#) (определение тома в пуле хранения)

[UPDATE MGMTCLASS](#) (обновление класса управления)

[UPDATE STGPOOL](#) (обновить пул хранения)

Защита сервера IBM Spectrum Protect

Защитите сервер IBM Spectrum Protect и данные, управляя доступом к серверам и клиентским узлам, шифруя данные и обеспечивая защищенные уровни прав доступа и пароли.

Управление администраторами

Администратор с системными полномочиями может выполнить любую задачу с сервером IBM Spectrum Protect, включая назначение уровней полномочий для других администраторов. Чтобы выполнить ряд задач, вам должны быть предоставлены полномочия путем назначения одного или нескольких уровней полномочий.

Процедура

Чтобы изменить параметры администратора, выполните описанные ниже шаги.

Задача	Процедура
Добавить администратора	<p>Чтобы добавить администратора, ADMIN1, с системными полномочиями и задать пароль, выполните следующие шаги:</p> <ol style="list-style-type: none">а. Зарегистрируйте администратора и задайте Pa\$#\$tw0 в качестве пароля, введя следующую команду: <pre>register admin admin1 Pa\$#\$tw0</pre>б. Предоставьте администратору системные полномочия, введя следующую команду: <pre>grant authority admin1 classes=system</pre>

Задача	Процедура
Изменить административные полномочия	<p>Измените уровень полномочий для администратора ADMIN1.</p> <ul style="list-style-type: none"> Предоставьте администратору системные полномочия, введя следующую команду: <pre>grant authority admin1 classes=system</pre> Аннулируйте системные полномочия администратора, введя следующую команду: <pre>revoke authority admin1 classes=system</pre>
Удалить администраторов	<p>Аннулируйте для администратора ADMIN1 доступ к серверу IBM Spectrum Protect, введя следующую команду:</p> <pre>remove admin admin1</pre>
Временно запретите доступ к серверу	<p>Заблокируйте или разблокируйте администратора, введя команду LOCK ADMIN или UNLOCK ADMIN.</p>

Понятия, связанные с данным

[Планирование ролей администратора](#)

Задайте уровень полномочий, которые вы хотите назначить для решения IBM Spectrum Protect.

Изменение требований к паролям

Можно изменить минимальный предел пароля, длину пароля, срок действия пароля, а также включить или выключить аутентификацию для IBM Spectrum Protect.

Об этой задаче

Применяя аутентификацию на основе паролей и управляя ограничениями паролей, вы защищаете данные и серверы от потенциальных угроз безопасности.

Процедура

Чтобы изменить требования к паролям для серверов IBM Spectrum Protect, выполните описанные ниже задачи.

Таблица 36. Задачи по аутентификации для серверов IBM Spectrum Protect	
Задача	Процедура
Задать максимальное число попыток ввода неправильного пароля.	<ol style="list-style-type: none"> Выберите сервер на странице Серверы Центра операций. Щелкните по Сведения, а затем по вкладке Свойства. Задайте число неудачных попыток в поле Предел неудачных попыток входа в систему. Значение по умолчанию при установке равно 0.

Таблица 36. Задачи по аутентификации для серверов IBM Spectrum Protect (продолжение)

Задача	Процедура
Задайте минимальную длину пароля.	<ul style="list-style-type: none"> a. Выберите сервер на странице Серверы Центра операций. b. Щелкните по Сведения, а затем по вкладке Свойства. c. Задайте число символов в поле Минимальная длина пароля.
Задайте срок действия паролей.	<ul style="list-style-type: none"> a. Выберите сервер на странице Серверы Центра операций. b. Щелкните по Сведения, а затем по вкладке Свойства. c. Задайте срок в днях в поле Общий срок действия паролей.
Отключите аутентификацию на основе паролей.	<p>По умолчанию сервер автоматически использует аутентификацию с помощью пароля. При аутентификации пароля все пользователи для получения доступа к серверу должны вводить пароль.</p> <p>Запретить аутентификацию пароля можно только для паролей, аутентификация которых выполняется на сервере (LOCAL). Отключая аутентификацию на основе паролей, вы делаете сервер доступным для угроз безопасности.</p>
Задать метод аутентификации по умолчанию.	<p>Введите команду SET DEFAULTAUTHENTICATION. Например, чтобы использовать сервер как метод аутентификации по умолчанию, введите следующую команду:</p> <pre>set defaultauthentication local</pre> <p>Чтобы обновить клиентский узел для аутентификации на сервере, включите AUTHENTICATION=LOCAL в команду UPDATE NODE:</p> <pre>update node authentication=local</pre>

Защита сервера в системе

Защитите систему, в которой сервер IBM Spectrum Protect работает, чтобы предотвратить несанкционированный доступ.

Процедура

Убедитесь, что неавторизованные пользователи не могут получить доступ к каталогам для базы данных сервера и экземпляра сервера. Оставьте для этих каталогов параметры доступа, которые вы сконфигурировали во время реализации.

Ограничение доступа пользователей к серверу

Уровни полномочий определяют то, что администратор может сделать с сервером IBM Spectrum Protect. Администратор с системными полномочиями может выполнить любую задачу на сервере. Администраторы, обладающие полномочиями политики, хранения или оператора, могут выполнять только определенный набор задач.

Процедура

1. После регистрации администратора с использованием команды **REGISTER ADMIN** используйте команду **GRANT AUTHORITY**, чтобы задать уровень полномочий администратора.
Дополнительные сведения о том, как задавать и изменять полномочия, смотрите в разделе [“Управление администраторами”](#) на стр. 218.
2. Чтобы управлять полномочиями администратора на выполнение некоторых задач, используйте следующие две опции сервера:
 - а) Вы можете задать уровень полномочий, который должен быть у администратора, чтобы он мог ввести команды **QUERY** и **SELECT** с опцией сервера **QUERYAUTH**. По умолчанию, не требуется никакого уровня полномочий. Данное требование можно изменить, указав один из уровней полномочий, включая системные.
 - б) Вы можете указать, что для команд, которые заставляют сервер записывать внешний файл за счет использования серверной опции **REQSYSAUTHOUTFILE**, требуются системные полномочия. По умолчанию, для выполнения таких команд необходимы системные полномочия.
3. Можно ограничить резервное копирование данных на клиентском узле, так чтобы его могли выполнять только ID пользователя root или авторизованные пользователи.
Например, чтобы ограничить резервное копирование ID пользователя root, введите команду **REGISTER NODE** или **UPDATE NODE** и задайте параметр **BACKUPINITIATION=root**:

```
update node backupinitiation=root
```

Остановка и запуск сервера

Прежде чем выполнять задачи по обслуживанию или переконфигурированию, остановите сервер. Затем запустите сервер в режиме обслуживания. Когда завершите задачи по обслуживанию или переконфигурированию, перезапустите сервер в производственном режиме.

Прежде чем начать

Чтобы остановить и запустить сервер IBM Spectrum Protect, требуются системные полномочия или полномочия оператора.

Остановка сервера

Прежде чем остановить сервер, подготовьте систему, проследив, чтобы все операции по резервному копированию базы данных были завершены и чтобы все прочие процессы и сеансы были закончены. Благодаря этому, вы сможете безопасным образом завершить работу сервера и обеспечить защиту данных.

Об этой задаче

При вводе команды **HALT** для остановки сервера происходят следующие действия:

- Все процессы и сеансы узлов клиентов будут отменены.
- Все текущие транзакции будут остановлены. (При перезапуске сервера будет произведен откат транзакций.)

Процедура

Чтобы подготовить систему и остановить сервер, выполните следующие шаги:

1. Запретите запуск новых сеансов клиентских узлов, введя команду **DISABLE SESSIONS**:

```
disable sessions all
```

2. Определите, не выполняются ли какие-либо сеансы клиентских узлов или процессы, выполнив следующее:

- a. На странице Центра операций **Обзор** посмотрите в области **Активность** общее число процессов и сеансов, которые активны в настоящий момент. Если это число заметно отличается от значения, которое обычно показано во время повседневного управления хранением, то просмотрите другие индикаторы состояния в Центре операций, чтобы определить, ошибка ли это.

- b. Смотрите график в области **Активность**, чтобы сравнить объем сетевого трафика за следующие периоды:

- Текущий период, то есть, самые последние 24 часа
- Предыдущий период, то есть, за 24 часа до текущего периода

Если на графике за предыдущий период показано ожидаемый объем трафика, существенные различия с графиком за текущий период могут указывать на проблему.

- c. Выберите на странице **Серверы** сервер, для которого вы хотите посмотреть процессы и сеансы, и щелкните по **Сведения**. Если сервер не зарегистрирован как хаб или подчиненный сервер в Центре операций, получите информацию о процессах при помощи команд администрирования. Введите команду **QUERY PROCESS** для запроса процессов и получения информации о сеансах при помощи команды **QUERY SESSION**.

3. Дождитесь завершения сеансов клиентских узлов или отмените их. Чтобы отменить процессы и сеансы, сделайте следующее:

- Выберите на странице **Серверы** сервер, для которого вы хотите посмотреть процессы и сеансы, и щелкните по **Сведения**.
- Щелкните по вкладке **Активные задачи** и выберите один или несколько процессов, сеансов или комбинацию процессов и сеансов, которые вы хотите отменить.
- Нажмите кнопку **Отмена**.
- Если сервер не зарегистрирован как хаб или подчиненный сервер в Центре операций, отмените сеансы при помощи команд администрирования. Введите команду **CANCEL SESSION**, чтобы отменить сеанс и процессы при помощи команды **CANCEL PROCESS**.

Совет: Если процесс, который вы хотите отменить, ожидает монтирования ленточного тома, требование монтирования будет отменено. Например, если вы введете команду **EXPORT**, **IMPORT** или **MOVE DATA**, команда может инициировать процесс, для которого потребуется смонтировать ленточный том. Однако, если ленточный том монтируется автоматизированной библиотекой, операция отмены может не иметь силы, пока не завершится процесс монтирования. В зависимости от вашей системной среды на это может потребоваться несколько минут.

4. Остановите сервер с помощью команды **HALT**:

```
halt
```

Запуск сервера для задач обслуживания или реконфигурирования

Прежде чем приступить к выполнению задач по обслуживанию или переконфигурированию, запустите сервер в режиме обслуживания. При запуске сервера в режиме обслуживания вы отключаете операции, которые могут помешать задачам обслуживания или переконфигурирования.

Об этой задаче

Запустите сервер в режиме обслуживания, запустив утилиту **DSMSERV** с параметром **MAINTENANCE**.

В режиме обслуживания отключаются следующие операции:

- Расписания выполнения административных команд
- Клиентские расписания
- Восстановление пространства хранения на сервере
- Устаревание инвентарного перечня
- Перенастройка пулов хранения

Кроме того, клиентам запрещено запускать сеансы с сервера.

Советы:

- Чтобы запустить сервер в режиме обслуживания, не нужно изменять файл опций сервера, `dsmserve.opt`.
- Когда сервер работает в режиме обслуживания, вы можете вручную запустить восстановление пространства хранения, истечение срока действия перечня и процессы переноса пулов хранения.

Процедура

- Чтобы запустить сервер в режиме обслуживания, введите следующую команду:

```
dsmserve maintenance
```

Совет: Видеоклип, иллюстрирующий запуск сервера в режиме обслуживания, смотрите на веб-странице [Запуск сервера в режиме обслуживания](#).

Дальнейшие действия

Чтобы возобновить операции сервера в производственном режиме, выполните следующие шаги:

1. Завершите работу сервера с помощью команды **HALT**:

```
halt
```

2. Запустите сервер, используя метод, который вы используете в производственном режиме. Выполните инструкции для вашей операционной системы.

- **AIX** [Запуск экземпляра сервера](#)
- **Linux** [Запуск экземпляра сервера](#)
- **Windows** [Запуск экземпляра сервера](#)

Операции, которые были отключены во время режима обслуживания, будут снова включены.

Планирование обновления сервера

Когда станет доступен пакет исправлений или промежуточное исправление, вы сможете обновить сервер IBM Spectrum Protect, чтобы воспользоваться преимуществами в улучшенном продукте. Серверы и клиенты можно обновлять в разное время. Перед обновлением сервера убедитесь, что вы выполнили шаги по планированию.

Об этой задаче

Выполните следующие рекомендации:

- Предпочтительный метод - обновить сервер с использованием мастера установки. Запустив мастер, щелкните в окне **IBM Installation Manager** по значку **Обновить**; не щелкайте по значкам **Установить** и **Изменить**.
- Если доступны обновления и для серверного компонента, и для компонента Центр операций, выберите переключатели, указывающие, что нужно обновить оба компонента.

Процедура

1. Проверьте список пакетов исправлений и промежуточных исправлений. Смотрите раздел [Скачивания IBM Spectrum Protect - последние пакеты исправлений и временные исправления](#).
2. Ознакомьтесь с усовершенствованиями продукта, описанными в файлах readme.
Совет: Получив пакет установки со страницы [Сайт поддержки IBM Spectrum Protect](#), вы также сможете получить доступ к файлу readme.
3. Убедитесь что версия, до которой вы обновляете сервер, совместима с другими компонентами, например, с агентами хранения и клиентами библиотек. Смотрите раздел [Совместимость агента хранения и библиотечного клиента с сервером IBM Spectrum Protect](#).
4. Если ваше решение включает в себя серверы или клиенты с более ранним уровнем версии, чем V7.1, смотрите рекомендации, чтобы убедиться, что операции резервного копирования и архивирования клиента не будут нарушены. Смотрите раздел [Замечания о совместимости и обновлении IBM Spectrum Protect](#).
5. Прочтите инструкции по обновлению. Обязательно создайте резервную копию базы данных сервера, информации о конфигурации устройств и файла хронологии томов.

Дальнейшие действия

Чтобы установить пакет исправлений или промежуточное исправление, следуйте инструкциям для вашей операционной системы:

- **AIX** [Установка пакета fix рас для сервера IBM Spectrum Protect](#)
- **Linux** [Установка пакета fix рас для сервера IBM Spectrum Protect](#)
- **Windows** [Установка пакета fix рас для сервера IBM Spectrum Protect](#)

Подготовка к отключению или обновлению системы

Подготовьте IBM Spectrum Protect, чтобы при плановом отключении питания или обновлении системы сохранять вашу систему в непротиворечивом состоянии.

Об этой задаче

Убедитесь, что вы запланировали регулярные действия по управлению, защите и обслуживанию сервера. Информацию о таких операциях планирования, как резервное копирование базы данных, резервное копирование файлов конфигурации устройств и резервное копирование хронологии томов, смотрите в разделе [“Как задать расписания для операций по обслуживанию сервера”](#) на стр. 62.

Процедура

1. Отмените выполняющиеся процессы и сеансы, сделав следующее:
 - a. Выберите в Центре операций на странице **Серверы** сервер, для которого вы хотите посмотреть процессы и сеансы, и щелкните по **Сведения**.
 - b. Щелкните по вкладке **Активные задачи** и выберите один или несколько процессов, сеансов или комбинацию процессов и сеансов, которые вы хотите отменить.
 - c. Нажмите кнопку **Отмена**.

2. Остановите сервер с помощью команды **HALT**:

```
halt
```

Совет: Можно ввести команду halt из Центра операций, установив указатель мыши на значок **Параметры** и щелкнув по **Построитель команд**. Затем выберите сервер, введите halt и нажмите на клавишу ввода (**Enter**).

Информация, связанная с данной

HALT (выключение сервера)

Подготовка к аварии и восстановление после аварии с использованием DRM

В IBM Spectrum Protect есть функция disaster recovery manager (DRM) для восстановления данных сервера и клиента при аварии.

DRM отслеживает перемещение носителей вне площадки и регистрирует эту информацию в базе данных IBM Spectrum Protect. DRM объединяет планы, сценарии и другую информацию в файле плана, который необходим для восстановления сервера IBM Spectrum Protect в случае, если произойдет авария или незапланированное отключение электричества. Если вас беспокоят возможные атаки вредоносных программ, включая программы, требующие выкупа, рассмотрите возможность использовать DRM, так как эта функция поможет вам восстановить серверы после атаки.

Ограничение: DRM доступен только в продукте IBM Spectrum Protect Extended Edition.

Файл плана аварийного восстановления

В файле плана аварийного восстановления содержится информация, необходимая для восстановления сервера IBM Spectrum Protect до состояния, в котором он находился на момент выполнения последней операции резервного копирования базы данных, выполненной перед созданием плана.

План поделен на разделы, которые можно распределить по нескольким файлам. Каждый раздел содержит оператор begin и оператор end.

Таблица 37. Разделы файла плана аварийного восстановления	
Раздел	Информация в разделе
SERVER.REQUIREMENTS	Задаёт требования к пространству хранения для базы данных и журнала восстановления сервера.
RECOVERY.INSTRUCTIONS.GENERAL	Содержит инструкции, которые администратор ввел в файл, идентифицируемый префиксом RECOVERY.INSTRUCTIONS.GENERAL. Инструкции содержат стратегию восстановления, имена основных контактных лиц, обзор главных приложений, резервные копии которых были созданы на этом сервере, а также другие важные инструкции по восстановлению.
RECOVERY.INSTRUCTIONS.OFFSITE	Содержит инструкции, которые администратор ввел в файл, идентифицируемый префиксом RECOVERY.INSTRUCTIONS.OFFSITE. Инструкции задают имя и положение дистанционного хранилища, а также контактная информация администратора хранилища (например, имя и номер телефона).

Таблица 37. Разделы файла плана аварийного восстановления (продолжение)

Раздел	Информация в разделе
RECOVERY.INSTRUCTIONS.INSTALL	Содержит инструкции, которые администратор ввел в файл, идентифицируемый префиксом RECOVERY.INSTRUCTIONS.INSTALL. Инструкции содержат указания по восстановлению сборки базового сервера и сведения о расположении резервных копий образа системы.
RECOVERY.INSTRUCTIONS.DATABASE	Содержит инструкции, которые администратор ввел в файл, идентифицируемый префиксом RECOVERY.INSTRUCTIONS.DATABASE. Инструкции содержат указания по подготовке к восстановлению базы данных. Например, можно указать инструкции по инициализации или загрузке резервных томов для автоматизированной библиотеки. Примеров этого раздела нет.
RECOVERY.INSTRUCTIONS.STGPOOL	Содержит инструкции, которые администратор ввел в файл, идентифицируемый префиксом RECOVERY.INSTRUCTIONS.STGPOOL. Инструкции содержат названия приложений и имена пулов хранения копий, содержащих резервные копии этих приложений. Примеров этого раздела нет.
RECOVERY.VOLUMES.REQUIRED	Позволяет получить список томов пула хранения резервных копий базы данных и копий, которые нужны для восстановления сервера. Том резервной копии базы данных добавляется в список, если он является частью самой последней последовательности резервных копий базы данных. Том пула хранения копий добавляется в список, если он не пуст и не отмечен как поврежденный (destroyed).
RECOVERY.DEVICES.REQUIRED	Содержит сведения об устройствах, необходимых для чтения резервных томов.
RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE	Содержит сценарий с командами, необходимыми для восстановления сервера.
RECOVERY.SCRIPT.NORMAL.MODE	Содержит сценарий с командами, необходимыми для восстановления первичных пулов хранения сервера.
DB.STORAGEPATHS	Задаёт каталоги для базы данных IBM Spectrum Protect.
LICENSE.REGISTRATION	Содержит макрокоманду для регистрации серверных лицензий.
COPYSTGPOOL.VOLUMES.AVAILABLE	Содержит макрокоманду, позволяющую отмечать тома пулов хранения копий, которые были перемещены в удаленную систему хранения, а затем возвращены в подключенное положение. Эту информацию можно использовать в качестве руководства по командам администрирования. Можно также скопировать, изменить и запустить макрокоманду в файле. Эту макрокоманду вызывает сценарий RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
COPYSTGPOOL.VOLUMES.DESTROYED	Содержит макрокоманду, позволяющий пометить как недоступные тома пулов хранения копий, которые на момент аварии находились в подключенном расположении. Предполагается, что эти тома находятся в дистанционном хранилище и во время аварии не были повреждены. Эти сведения можно использовать в качестве руководства для ввода команд администрирования в командной строке; можно также скопировать их в файл, изменить его, а затем запустить макрокоманду. Эту макрокоманду вызывает сценарий RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
PRIMARY.VOLUMES.DESTROYED	Содержит макрокоманду, обозначающую находившиеся на момент аварии в подключенном расположении тома первичных пулов хранения как поврежденные (destroyed). Эти сведения можно использовать в качестве руководства для ввода команд администрирования в командной строке; можно также скопировать их в файл, изменить его, а затем запустить макрокоманду. Эту макрокоманду вызывает сценарий RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.

Таблица 37. Разделы файла плана аварийного восстановления (продолжение)	
Раздел	Информация в разделе
PRIMARY.VOLUMES.REPLACEMENT	Содержит макрокоманду для определения первичных пулов хранения замены. Эти сведения можно использовать в качестве руководства для ввода команд администрирования в командной строке; можно также скопировать их в файл, изменить его, а затем запустить макрокоманду. Эту макрокоманду вызывает сценарий RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
STGPOOLS.RESTORE	Содержит макрокоманду для восстановления первичных пулов хранения. Этот раздел можно использовать в качестве руководства, а административные команды вводить в командной строке. Можно также скопировать, изменить и запустить информацию в файле. Эта макрокоманда запускается сценарием RECOVERY.SCRIPT.NORMAL.MODE.
VOLUME.HISTORY.FILE	Содержит копию сведений об хронологии томов на момент создания плана восстановления. Файл хронологии томов используется утилитой DSMSERV RESTORE DB , чтобы определить, какие тома необходимы для восстановления базы данных. Файл хронологии томов используется сценарием RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
DEVICE.CONFIGURATION.FILE	Содержит копию данных о конфигурации устройств на момент создания плана восстановления. Файл конфигурации устройств используется утилитой DSMSERV RESTORE DB для чтения томов резервных копий базы данных. Файл конфигурации устройств используется сценарием RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
DSMSERV.OPT.FILE	Содержит копию файла серверных параметров. Этот раздел используется сценарием RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
LICENSE.INFORMATION	Содержит копию результатов последнего аудита лицензий, а также условия соглашения о лицензии на сервер.
MACHINE.GENERAL.INFORMATION	Позволяет получить информацию о компьютере сервера, например, его расположение, которое необходимо, чтобы перестроить компьютер сервера. Этот раздел содержится в файле плана, если сведения о компьютерах были сохранены в базе данных при помощи команды DEFINE MACHINE с параметром ADSMSEVER=YES .
MACHINE.RECOVERY.INSTRUCTIONS	Содержит инструкции по восстановлению для компьютера сервера. Этот раздел содержится в файле плана, если в базе данных были сохранены инструкции по восстановлению компьютера.
MACHINE.RECOVERY.CHARACTERISTICS	Содержит сведения о программных и аппаратных характеристиках сервера. Этот раздел содержится в файле плана, если характеристики компьютера сохранены в базе данных.
MACHINE.RECOVERY.MEDIA	Предоставляет информацию о носителях, необходимых для перестройки компьютера, содержащего сервер. Этот раздел содержится в файле плана, если сведения о носителях для восстановления сохранены в базе данных и связаны с компьютером, на котором расположен сервер.

Восстановление данных сервера и клиента с использованием DRM

Используйте функцию disaster recovery manager (DRM), чтобы восстановить данные сервера и клиента IBM Spectrum Protect, если произойдет авария.

Прежде чем начать

IBM Spectrum Protect настраивается для использования протокола Secure Sockets Layer (SSL) для аутентификации клиента/сервера. При запуске сервера создается файл цифрового сертификата,

cert.kdb как часть процесса. В этом файле содержится открытый ключ сервера, который позволяет клиенту шифровать данные. Файл цифрового сертификата не может храниться в базе данных сервера, поскольку для Global Security Kit (GSKit) необходим отдельный файл в определенном формате.

1. Сохраните резервные копии файлов cert.kdb, cert.sth и cert256.arm.
2. Если и исходные файлы сертификатов, и все копии окажутся потеряны или повреждены, сгенерируйте новый файл сертификата.

Главный ключ шифрования хранится в новой базе данных ключей, управляемой комплектом GSKit, dsmkeydb.kdb. Если на сервере есть существующий главный ключ шифрования, этот главный ключ шифрования будет перенесен из файла dsmseiv.pwd в базу данных ключей, dsmkeydb.kdb. Сохраните резервные копии файлов dsmkeydb.kdb и dsmkeydb.sth. Можно сконфигурировать команду **BACKUP DB** для резервного копирования главного ключа шифрования или можно самостоятельно создать резервную копию файлов dsmkeydb.kdb и dsmkeydb.sth вручную. Без главного ключа шифрования произвести восстановление после аварии будет невозможно.

1. Сохраните резервные копии файлов dsmkeydb.kdb и dsmkeydb.sth.

Процедура

1. Получите последний план восстановления.
2. Ознакомьтесь с этапами восстановления, описанными в разделе плана RECOVERY.INSTRUCTIONS.GENERAL.
3. Разбейте разделы файла плана по отдельным файлам, чтобы получить общие предварительные инструкции, сценарии восстановления сервера IBM Spectrum Protect и инструкции по восстановлению клиентов.
4. Получите все необходимые тома восстановления (как указано в плане) из хранилища.
5. Проверьте файл конфигурации устройств и убедитесь, что конфигурация оборудования на площадке восстановления совпадает с конфигурацией на исходной площадке. При наличии любых изменений следует соответствующим образом обновить файл конфигурации устройств. Ниже приведены примеры изменений, для которых нужно изменить конфигурацию:
 - Различные имена устройств.
 - Для автоматизированных библиотек - требование вручную разместить тома резервных копий базы данных в автоматизированной библиотеке и обновить данные о конфигурации для идентификации элементов библиотеки. Это позволит серверу находить расположение требуемых томов резервных копий базы данных.
6. Настройте замену оборудования для сервера IBM Spectrum Protect, включая операционную систему и установку базового выпуска IBM Spectrum Protect.
7. Запустите сценарий восстановления сервера IBM Spectrum Protect из плана восстановления. Разделы RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE и RECOVERY.SCRIPT.NORMAL.MODE содержат выполняемые файлы команд, которые можно использовать для управления восстановлением сервера IBM Spectrum Protect, вызывая другие файлы команд, сгенерированные в плане. Сценарий RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE восстанавливает сервер до той точки, в которой клиенты могут начать восстановление непосредственно с томов пулов хранения копий.
8. Восстановите первичные пулы хранения, используя сценарий RECOVERY.SCRIPT.NORMAL.MODE.
9. Запустите операции восстановления клиента в соответствии с порядком приоритетов, заданным в высокоуровневом планировании.

Дальнейшие действия

Теперь сервер IBM Spectrum Protect можно использовать для выполнения обычных операций сервера. Убедитесь, что запланированы все необходимые операции. Инструкции смотрите в разделах [“Как задать расписания для операций по обслуживанию сервера”](#) на стр. 62 и [Планирование операций резервного копирования и архивирования](#).

Информация, связанная с данной

PREPARE (создание файла с планом восстановления)

Исправление и восстановление данных в пулах хранения каталогов-контейнеров

Тренировка по восстановлению после аварий

Запланируйте отработку аварийного восстановления, чтобы подготовиться к аудиту, удостоверяющему возможность восстановления сервера IBM Spectrum Protect и гарантирующему, что можно восстановить данные и возобновить операции после перебоя с питанием. Отработка также поможет вам убедиться, что можно восстановить все данные и возобновить операции, прежде чем возникнет критическая ситуация.

Прежде чем начать

Выполните следующие задачи:

- Регулярно планируйте операции по управлению, защите и обслуживанию сервера. Дополнительную информацию о планировании смотрите в разделе [“Как задать расписания для операций по обслуживанию сервера”](#) на стр. 62. Убедитесь, что вы запланировали следующие задачи:
 - Резервное копирование базы данных.
 - Перемещение носителей вне площадки.
 - Резервное копирование файла конфигурации устройств, файла хронологии томов и файла опций сервера `dsmsevr.opt`.
 - **Необязательно:** Ввод команды **PREPARE** для создания файла плана аварийного восстановления.

Совет:

При вводе команды **PREPARE** функция IBM Spectrum Protect disaster recovery manager (DRM) создает одну копию файла плана аварийного восстановления.

Управлять аварийным восстановлением вне площадки можно, не используя DRM, однако DRM помогает консолидировать планы, сценарии и другую информацию, которая требуется при восстановлении после аварий.

Для безопасности создайте несколько копий плана. Например, сохраните копии в печатном виде, на флэш-накопителе USB, на дисковом пространстве вне площадки или на удаленном сервере. Файл плана аварийного восстановления ежедневно перемещается за пределы площадки с использованием лент. Дополнительную информацию о DRM смотрите в разделе [“Подготовка к аварии и восстановление после аварии с использованием DRM”](#) на стр. 225.

- Сконфигурируйте следующие ресурсы на площадке аварийного восстановления:
 1. Сервер IBM Spectrum Protect восстановления. Сервер на площадке аварийного восстановления должен относиться к тому же уровню, что и сервер на производственной площадке.
 2. Ленточную библиотеку для хранения носителей, поставляемых с производственной площадки. Дополнительную информацию о расположениях восстановления вне площадки смотрите в разделе [“Хранение данных вне площадки”](#) на стр. 26.
 3. Дисковое пространство хранения для базы данных, архивного журнала, активных журналов и пулов хранения.
 4. Клиенты для проверки операций по восстановлению.

Об этой задаче

Почаще проверяйте план аварийного восстановления и возможность восстановления сервера IBM Spectrum Protect в среде, аналогичной производственной среде.

Процедура

1. Убедитесь, что ленты доступны на площадке. Введите команду **QUERY LIBVOLUME**, чтобы идентифицировать тома, активируемые в автоматизированной библиотеке.
2. Создайте резервную копию базы данных на лентах на площадке, выполнив следующие шаги:
 - a. На странице **Серверы** в компоненте Центр операций выберите сервер, для базы данных которого вы хотите создать резервную копию.
 - b. Щелкните по **Резервное копирование** и выполните инструкции в окне **Резервное копирование базы данных**.
3. Скопируйте в домашний каталог сервера на площадке восстановления следующие файлы:
 - Файл плана аварийного восстановления
 - Файл хронологии тома
 - Файл конфигурации устройств
 - Необязательно: файл опций сервера `dsmseiv.opt`
4. Переместите ленту в расположение восстановления вне площадки.
5. Восстановите базу данных сервера, используя утилиту **DSMSERV RESTORE DB** на сервере восстановления.
6. Введите команду **UPDATE VOLUME** и задайте параметр **ACCESS=DESTROYED**, чтобы указать, что нужно восстановить весь том.
7. На сервере восстановления восстановите тома пула хранения при помощи команды **RESTORE STGPOOL**.

Дальнейшие действия

Убедитесь, что вы можете получить доступ к данным в библиотеке, произведя аудит ленточного тома в восстановленном пуле хранения, чтобы удостовериться, что данные не противоречивы. Чтобы произвести аудит ленточного тома, введите команду **AUDIT VOLUME**. Чтобы обеспечить более высокую производительность, произведите аудит только восстановленных данных.

Задачи, связанные с данной

Аудит перечня томов в библиотеке

Можно выполнить аудит автоматизированной библиотеки, чтобы обеспечить соответствие инвентарного списка томов библиотеки и томов, которые физически в ней находятся. Можно выполнить аудит библиотеки в случае нарушения целостности перечня томов библиотеки из-за перемещения томов в библиотеке вручную или в связи с ошибками базы данных.

Информация, связанная с данной

AUDIT VOLUME (проверка информации о томе пула хранения, содержащейся в базе данных)

DSMSERV RESTORE DB (восстановление базы данных)

RESTORE STGPOOL (восстановление данных в пуле хранения)

Восстановление базы данных

Если у вас включена функция disaster recovery manager (DRM) и вы выполнили процедуру по подготовке к аварии, вы сможете восстановить базу данных после аварии. Если у вас не сконфигурирована функция DRM, вы все равно сможете восстановить базу данных при условии, что у вас есть необходимые файлы резервных копий.

Прежде чем начать

Если каталоги базы данных и журнала восстановления потеряны, то создайте их заново, прежде чем вводить серверную утилиту **DSMSERV RESTORE DB**.

Об этой задаче

Вы можете восстановить базу данных до наиболее актуального состояния или на указанный момент времени. Чтобы восстановить базу данных на момент, когда она была потеряна, восстановите ее до самой последней версии.

ограничения:

- Чтобы восстановить базу данных до ее последней версии, нужно найти каталог архивного журнала. Если вы не сможете найти каталог, вам удастся восстановить базу данных только на конкретный момент времени.
- Протокол Secure Sockets Layer (SSL) нельзя использовать для операции восстановления баз данных.
- Вы не сможете восстановить базу данных сервера, если уровень выпуска резервной копии базы данных отличается от уровня выпуска восстанавливаемого сервера. Например, если вы используете сервер версии 8.1 и попытаетесь восстановить базу данных версии 7.1, произойдет ошибка.

Процедура

Чтобы восстановить базу данных, используйте серверную утилиту **DSMSERV RESTORE DB**. Выберите один из следующих методов в зависимости от того, какую версию базы данных вы хотите восстановить:

- Восстановить базу данных до самой последней версии. Например, введите следующую команду:

```
dsmserve restore db
```

- Восстановить базу данных на определенный момент времени. Например, чтобы восстановить базу данных на момент создания набора резервных копий от 19 апреля 2017 г., используйте следующую команду:

```
dsmserve restore db todate=04/19/2017
```

Информация, связанная с данной

[DSMSERV RESTORE DB \(восстановление базы данных\)](#)

Приложение А. Специальные возможности для семейства продуктов IBM Spectrum Protect

Специальные возможности помогают пользователю с физическими недостатками, например, с ограниченной подвижностью или с недостатками зрения, с успехом пользоваться продуктами информационных технологий.

Обзор

Продукты семейства IBM Spectrum Protect поддерживают следующие основные специальные возможности:

- Работа с использованием только клавиатуры
- Операции с использованием программы для чтения информации с экрана

Семейство продуктов IBM Spectrum Protect использует новейший стандарт W3C, [WAI-ARIA 1.0](http://www.w3.org/TR/wai-aria/) (www.w3.org/TR/wai-aria/), чтобы обеспечить соответствие разделу [US Section 508](http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/) (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/) и рекомендациям по доступности веб-содержимого ([Web Content Accessibility Guidelines \(WCAG\) 2.0](http://www.w3.org/TR/WCAG20/) (www.w3.org/TR/WCAG20/)). Чтобы воспользоваться преимуществами специальных возможностей, возьмите последний выпуск вашей программы чтения информации с экрана и последний веб-браузер, поддерживаемый продуктом.

Документация по продукту в центре знаний IBM включена для поддержки специальных возможностей. Специальные возможности центра знаний IBM описаны в разделе [Специальные возможности справки по центру знаний IBM](http://www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility) (www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility).

Управление при помощи клавиатуры

Для управления этим продуктом используются стандартные комбинации клавиш.

Информация об интерфейсе

В пользовательских интерфейсах нет содержимого, которое бы мигало 2-55 раз в секунду.

В пользовательских веб-интерфейсах правильное воспроизведение содержимого и подходящий для работы режим основаны на каскадных таблицах стилей. Приложение обеспечивает пользователям со слабым зрением эквивалентный способ использовать параметры системного дисплея, включая высококонтрастный режим. Можно управлять размером шрифта, используя параметры устройства или веб-браузера.

В пользовательских веб-интерфейсах есть навигационные отметки WAI-ARIA, которые позволяют быстро переходить к функциональным областям в приложении.

Программное обеспечение поставщиков

В семейство продуктов IBM Spectrum Protect включены программы некоторых поставщиков, на которые не распространяется лицензионное соглашение IBM. IBM не делает никаких заявлений относительно специальных возможностей этих продуктов. За информацией о специальных возможностях этих продуктов обращайтесь к их поставщикам.

Связанная информация о специальных возможностях

Помимо стандартной консультативно-справочной службы IBM и веб-сайтов поддержки у IBM есть две телефонные службы ТТУ для использования глухими или слабо слышащими заказчиками с целью получения доступа к службам продаж и поддержки:

Служба ТТУ
800-IBM-3383 (800-426-3383)
(в Северной Америке)

Дополнительную информацию об обязательствах, которые IBM принимает на себя в отношении поддержки специальных возможностей, смотрите на сайте [IBM Accessibility](http://www.ibm.com/able) (IBM - Специальные возможности) (www.ibm.com/able).

Замечания

Эта публикация разрабатывалась для продуктов и услуг, предлагаемых в США. Материалы на других языках можно получить в IBM. Однако для доступа к копии продукта или версии продукта вы должны быть владельцем копии или версии.

IBM может не предлагать описанные продукты, услуги и возможности в других странах. Сведения о продуктах и услугах, доступных в настоящее время в вашей стране, можно получить в местном представительстве IBM. Любые ссылки на продукты, программы или услуги IBM не означают явным или неявным образом, что можно использовать только продукты, программы или услуги IBM. Разрешается использовать любые функционально эквивалентные продукты, программы или услуги, если при этом не нарушаются права IBM на интеллектуальную собственность. Однако при этом пользователь сам несет ответственность за оценку и проверку работы с другими (не IBM) продуктами, программами и услугами.

Компания IBM может располагать патентами или рассматриваемыми заявками на патенты, относящимися к предмету данного документа. Получение этого документа не означает предоставления каких-либо лицензий на эти патенты. Запросы относительно лицензий направляйте по адресу:

*IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US*

По поводу лицензий, связанных с использованием наборов двухбайтных символов (DBCS), обращайтесь в отдел интеллектуальной собственности IBM в вашей стране или направьте запрос в письменной форме по адресу:

*Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan*

КОРПОРАЦИЯ INTERNATIONAL BUSINESS MACHINES ПРЕДОСТАВЛЯЕТ ДАННУЮ ПУБЛИКАЦИЮ "КАК ЕСТЬ", БЕЗ КАКИХ-ЛИБО ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ТАКОВЫМИ, ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ ОТСУТСТВИЯ НАРУШЕНИЙ, КОММЕРЧЕСКОЙ ПРИГОДНОСТИ ИЛИ СООТВЕТСТВИЯ КАКОЙ-ЛИБО КОНКРЕТНОЙ ЦЕЛИ. В некоторых законодательствах для определенных сделок подобные оговорки не допускаются, таким образом, это утверждение может не относиться к вам.

В данной информации могут встретиться технические неточности или типографские опечатки. В публикацию время от времени вносятся изменения, которые будут отражены в следующих изданиях. Фирма IBM может в любое время без уведомления вносить изменения и усовершенствования в продукты и программы, описанные в этой публикации.

Любые ссылки в этой публикации на сайты, не принадлежащие IBM, приведены только для удобства и никоим образом не означают их поддержки. Материалы на этих сайтах не входят в число материалов по данному продукту IBM, и весь риск пользования этими сайтами несете вы сами.

IBM оставляет за собой право на использование и распространение любой предоставленной вами информации любыми способами, какие сочтет приемлемыми, не принимая на себя никаких обязательств перед вами.

Если обладателю лицензии на данную программу понадобятся сведения о возможности: (i) обмена данными между независимо разработанными программами и другими программами (включая данную) и (ii) совместного использования таких данных, он может обратиться по адресу:

*IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US*

Такая информация может быть предоставлена при соблюдении определенных положений и условий и, возможно, за определенную плату.

Лицензированная программа, описанная в данном документе, и все лицензированные материалы, доступные с ней, предоставляются IBM на условиях IBM Customer Agreement (Соглашения IBM с заказчиком), Международного соглашения о лицензиях на программы IBM или эквивалентного соглашения.

Показанные здесь данные производительности получены в определенных условиях. Реальные результаты могут быть другими.

Информация о продуктах других компаний (не IBM) получена от поставщиков этих продуктов, из их опубликованных объявлений или из иных общедоступных источников. IBM не производила тестирование этих продуктов и никак не может подтвердить информацию о их точности работы и совместимости, а также прочие заявления относительно продуктов других компаний (не IBM). Вопросы о возможностях продуктов других компаний (не IBM) следует направлять поставщикам этих продуктов.

В этой публикации содержатся примеры данных и отчетов, используемых при выполнении текущих служебных задач. Чтобы проиллюстрировать эти задачи с максимальной наглядностью, в примерах используются имена физических лиц, названия компаний, фирм и продуктов. Все эти имена и названия вымышлены, и любое их сходство с реальными именами и адресами полностью случайно.

ЛИЦЕНЗИЯ НА ПРАВО КОПИРОВАНИЯ:

В этом документе содержатся примеры прикладных программ на языках программирования, которые иллюстрируют методы программирования для различных операционных платформ. Вы имеете право копировать, изменять и распространять эти примеры программ в любой форме без уплаты вознаграждения фирме IBM в целях разработки, применения, сбыта или распространения прикладных программ, соответствующих интерфейсу прикладных программ операционной системы, для которой предназначены эти примеры. Эти примеры не были тщательно протестированы при всех возможных условиях. Поэтому IBM не может гарантировать их надежность, пригодность и функционирование. Пробные программы предоставляются по принципу 'как есть', без какой-либо гарантии. IBM не несет ответственности ни за какой ущерб, возникший в результате использования примеров программ.

Каждая копия программ примеров или программ, созданных на их основе, должна содержать следующее замечание об авторских правах: © (название вашей компании) (год). Части этого кода построены на основе примеров программ IBM Corp. © Copyright IBM Corp. _введите год или годы_.

Товарные знаки

IBM, логотип IBM и ibm.com - товарные знаки или зарегистрированные товарные знаки International Business Machines Corporation, зарегистрированные во многих странах. Прочие названия продуктов и услуг могут быть товарными знаками IBM или других компаний. Текущий список товарных знаков IBM смотрите на веб-странице "Copyright and trademark information" (Информация об авторских правах и товарных знаках) (www.ibm.com/legal/copytrade.shtml).

Adobe - зарегистрированный товарный знак Adobe Systems Incorporated в США и/или в других странах.

Linear Tape-Open, LTO и Ultrium - товарные знаки HP, IBM Corp. и Quantum в США и в других странах.

Intel и Itanium - товарные знаки или зарегистрированные товарные знаки Intel Corporation или ее филиалов в США и/или других странах.

Linux - зарегистрированный товарный знак Линуса Торвальдса (Linus Torvalds) в США и/или других странах.

Microsoft, Windows и Windows NT - товарные знаки Microsoft Corporation в США и/или в других странах.

Java™ и все товарные знаки и логотипы на основе Java - это товарные знаки или зарегистрированные товарные знаки Oracle и/или аффилированных компаний Oracle.

UNIX - зарегистрированный товарный знак The Open Group в США и других странах.

VMware, VMware vCenter Server и VMware vSphere - это зарегистрированные товарные знаки или товарные знаки VMware, Inc. или подразделений VMware, Inc. в США и/или других зонах юрисдикции.

Положения и условия для документации по продукту

Разрешения на использование этих публикаций предоставляются при соблюдении нижеприведенных положений и условий.

Применимость

Указанные условия и положения добавляются ко всем условиям для веб-сайта IBM.

Личное использование

Вы можете воспроизводить эти публикации для своего личного некоммерческого использования при условии, что при этом будут соблюдены все замечания об имущественных правах. Не разрешается распространять, воспроизводить или составлять производные работы на основе данных публикаций или их частей без выраженного согласия IBM.

Коммерческое использование

Вам предоставляется право воспроизводить эти публикации исключительно в пределах своего предприятия при условии, что будут воспроизведены все замечания об авторских правах. За пределами вашего предприятия вам запрещается распространять эти публикации, полностью или по частям, демонстрировать их или создавать из них производные продукты без явного на то согласия от IBM.

Права

За исключением прав, явным образом предоставляемых настоящим разрешением, никаких иных разрешений, лицензий и прав, ни явных, ни подразумеваемых, в отношении публикаций и любой содержащейся в них информации, данных, программ или иной интеллектуальной собственности, не предоставляется.

IBM оставляет за собой право отозвать разрешения, предоставленные этим документом, если, по мнению IBM, использование публикаций наносит ущерб IBM или, как это установлено IBM, вышеприведенные инструкции не соблюдаются должным образом.

Вам не разрешается скачивать, экспортировать или повторно экспортировать эту информацию иначе, чем в полном соответствии с правилами и нормативами, включая все законы и правила Соединенных Штатов об экспорте.

IBM НЕ ПРЕДОСТАВЛЯЕТ НИКАКИХ ГАРАНТИЙ КАСАТЕЛЬНО СОДЕРЖИМОГО ЭТИХ ПУБЛИКАЦИЙ. ПУБЛИКАЦИИ ПРЕДСТАВЛЯЮТСЯ "КАК ЕСТЬ", БЕЗ КАКИХ-ЛИБО ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ (НО НЕ ОГРАНИЧИВАЯСЬ ТАКОВЫМИ) ПРЕДПОЛАГАЕМЫЕ ГАРАНТИИ РЫНОЧНОЙ ПРИГОДНОСТИ, НЕНАРУШЕНИЯ ПРАВ ИЛИ СООТВЕТСТВИЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ.

Замечания о политике конфиденциальности

В программных продуктах IBM, включая программы как решения служб ("Программные предложения"), могут использоваться cookies или другие технологии для сбора информации по

использованию продукта, чтобы помочь конечному пользователю в работе, настроить взаимодействия с конечным пользователем или для иных целей. Во многих случаях предложения ПО не собирают информацию, позволяющую идентифицировать личность. Некоторые наши предложения ПО могут помочь вам собрать информацию, позволяющую идентифицировать личность. Если данное предложение ПО использует cookies для сбора информации, позволяющей идентифицировать личность, то ниже будет приведена конкретная информация об использовании cookies в этом предложении.

Настоящее предложение ПО не использует cookies или иные технологии для сбора информации, позволяющей идентифицировать личность.

Если конфигурации, внедренные для этого Предложения относительно программ, обеспечивают вам, как заказчику, возможность собирать информацию, позволяющую идентифицировать личность, от конечных пользователей через cookies и другие технологии, вы должны обратиться за местной юридической рекомендацией о том, существуют ли какие-либо законы, применимые к такому сбору данных, включая все требования относительно предоставления замечаний и согласований.

Дополнительную информацию об использовании в этих целях различных технологий, включая cookies, смотрите на странице политики конфиденциальности IBM по адресу: <http://www.ibm.com/privacy>, и в заявлении IBM об электронной конфиденциальности (IBM's Online Privacy Statement) по адресу: <http://www.ibm.com/privacy/details>, в разделе, озаглавленном "Cookies, Web Beacons and Other Technologies" (Cookies, веб-маяки и другие технологии), а также в документе "IBM Software Products and Software-as-a-Service Privacy Statement" ((Программные продукты IBM и заявление о конфиденциальности программ как услуг) по адресу: <http://www.ibm.com/software/info/product-privacy>).

Глоссарий

Есть глоссарий с терминами и определениями для семейства продуктов IBM Spectrum Protect.

См. [IBM Spectrum Protect - Глоссарий](#).

Индекс

D

DEFINE DRIVE, команда [97](#)
DEFINE LIBRARY, команда [96](#)
DELETE DRIVE [216](#)
DISMOUNT VOLUME, команда [205](#)
DRM 67–69, [225](#), [227](#), [229](#), [230](#)
DSMSERV RESTORE DB [230](#)

I

IBM Spectrum Protectdisaster recovery manager [225](#), [227](#)
ID пользователя
 создать для сервера [45](#)

L

LDAP
 требования к паролям [219](#)

M

MOVE RETMEDIA [73](#), [74](#)

Q

QUERY SAN [137](#)

S

SAN (сеть хранения данных)
 доступ клиентов к устройствам [18](#), [20](#)
 изменения устройств, обнаружение [136](#)
 перемещение данных в режиме без сети (LAN-free data movement) [18](#), [20](#)
 роль агента хранения [18](#), [20](#)
 совместное использование библиотеки серверами [18](#), [105](#)
SCSI
 автоматическое присвоение меток томам [190](#)
 библиотека с разными ленточными технологиями [102](#)
server
 запуск в режиме обслуживания [221](#)
 обновление плана [223](#)
 остановка [221](#)
SSL [57](#)

T

TLS [57](#)
tsmdlst, утилита [137](#)

U

Ultrium, тип устройств LTO
 класс устройств, определение и обновление [99](#)
 шифрование [101](#), [129](#)
 WORM [137](#)

A

авария
 менеджер аварийного восстановления [225](#)
автоматизированная библиотека
 чистый том (scratch volume) [201](#)
авточейнджеры [88](#)
агент хранения [18](#), [20](#)
административные команды
 AUDIT LIBVOLUME [202](#)
 CHECKIN LIBVOLUME [191](#), [193](#)
 CHECKOUT LIBVOLUME [200](#)
 CLEAN DRIVE [212](#)
 DEFINE DEVCLASS
 3592 [102](#)
 классы устройств LTO [99](#)
 DEFINE DRIVE [97](#)
 DEFINE LIBRARY [96](#)
 UPDATE DRIVE [207](#), [208](#)
 UPDATE LIBVOLUME [200](#)
 UPDATE VOLUME [196](#)
 VALIDATE LANFREE [126](#)
адрес элемента [97](#), [195](#)
аппаратные средства хранения
 конфигурировать [34](#)
аудит
 перечень томов библиотеки [202](#)

Б

библиотека
 автоматизированный [199](#)
 аудит перечня томов [202](#)
 добавление томов [191](#)
 задать [96](#)
 конфигурация [94](#)
 настройка для нескольких типов устройств [21](#), [22](#)
 обнаружение изменений, в SAN [96](#), [136](#)
 перечень томов [203](#)
 режим, произвольный или последовательный [79](#)
 серийный номер [96](#)
 смешивание типов устройств [21](#), [22](#), [99](#), [102](#)
 совместное использование [17](#)
 совместное использование серверами [105](#)
 SCSI [17](#)
Библиотеки SCSI
 определить клиент библиотеки [106](#), [108](#)
 определить сервер библиотеки [106](#), [108](#)
брандмауэр [29](#)
брандмауэры

брандмауэры (*продолжение*)
конфигурирование связи через [125](#)

В

вне площадки, хранение [26](#)
внутреннее лицензирование мощности [164](#)
восстановление базы данных [230](#)
восстановление данных
стратегия [229](#)

Г

графический мастер
необходимые файлы RPM [50](#)

Д

данные
 деактивация [174](#)
диагностика устройства [137](#)
диагностика, для устройства [137](#)
домены политик
 задать [115](#)
драйвер ленточного устройств
 требования [79](#)
 установка [79](#)
драйвер устройств
 для устройств автоматизированной библиотеки [78](#)
 конфигурирование [88](#), [89](#), [92](#), [93](#)
 требования [78](#)
 установка [78](#)
 IBM Spectrum Protect, установка [78](#)
драйвер устройства IBM Spectrum Protect [79](#)
драйвер, ленточное устройство
 требования [79](#)
 установка [79](#)
драйверы ленточных устройств IBM [80](#)
драйверы устройств
 установка [82](#)
драйверы устройств IBM
 конфигурирование [83](#)
 установка [83](#)
Драйверы устройств IBM Spectrum Protect [80](#)
драйверы, устройство [83](#)

Е

ежедневный контрольный список задач мониторинга [143](#)
емкость активного журнала [174](#)
емкость архивного журнала [174](#)
емкость базы данных [174](#)
емкость перечня [174](#)
емкость пула хранения [2](#)
емкость томов [131](#)
емкость, лента [131](#)

Ж

журнал аварий [67–69](#), [225](#), [227](#), [229](#)
журналы ошибок
 оценка [167](#)

З

завершение работы
 server [221](#)
задать накопитель [217](#)
задачи обслуживания
 запуск сервера в режиме обслуживания [222](#)
 планирование [176](#)
задачи переконфигурирования
 запуск сервера в режиме обслуживания [222](#)
замена ленточного накопителя [216](#)
замена томов в автоматизированной библиотеке [194](#)
заменить накопитель [217](#)
запланированные действия
 настройка [176](#)
запуск сервера
 режим обслуживания [221](#)
защита
 шифрование данных
 3592 Generation 2 [104](#)
 IBM LTO, поколение 4 [129](#)
 IBM LTO, поколение 4 или новее [101](#)
 Oracle StorageTek T10000B [129](#)
 Oracle StorageTek T10000C [129](#)
 Oracle StorageTek T10000D [129](#)
 шифрование данных, 3592 Generation 2, TS1120, TS1130, TS1140, TS1150 [129](#)
защита данных [137](#)
защита данных с помощью носителей WORM [137](#)
защита логических блоков
 обзор [208](#)
 операции чтения/записи [211](#)
 поддерживаемые накопители [209](#)
 разрешение [210](#)
 управление пулами хранения [212](#)
защищенная связь
 конфигурирование SSL и TLS [57](#)

И

иерархии пулов хранения
 конфигурирование [111](#)
 планирование [23](#)
имена специальных файлов [81](#)
имя устройства [81](#)
имя файла для устройства [81](#)
интервал времени, настройка для регистрации томов [134](#)

К

картридж
 смешивание поколений накопителей [102](#)
 чистящий картридж [163](#), [215](#)
Каталоги компонента IBM Spectrum Protect
 планирование [8](#)
клавиатура [233](#)
класс привилегий (privilege class)
 системные полномочия [218](#)
класс устройства
 задать [98](#)
 параметр FORMAT [132](#)
 LTO [99](#)

клиент библиотеки, совместно используемая библиотека [18](#), [109](#)

клиенты

выбор программы [113](#)

добавление [112](#)

защита [112](#)

конфигурирование [121](#)

конфигурирование для выполнения

запланированных операций [122](#)

обновление [170](#)

определить расписания [78](#)

регистрация [120](#)

соединение с сервером [120](#)

управление операциями [167](#)

установка [121](#)

команда AUDIT LIBVOLUME [202](#)

команда CHECKIN LIBVOLUME [191](#), [192](#)

команда CHECKOUT LIBVOLUME [200](#)

команда CLEAN DRIVE [212](#), [215](#)

команда LABEL LIBVOLUME

идентификация накопителей [189](#)

использование устройства библиотеки [189](#)

маркировка томов пулов хранения с

последовательным доступом [189](#)

перезапись существующих меток тома [189](#)

примеры маркировки томов [189](#)

тома сменных носителей [189](#)

Команда UPDATE DRIVE [207](#), [208](#)

Команда UPDATE LIBVOLUME [200](#)

команда VALIDATE LANFREE [126](#)

команды

HALT [221](#)

команды, администрирование

AUDIT LIBVOLUME [202](#)

CHECKIN LIBVOLUME [191](#), [193](#)

CHECKOUT LIBVOLUME [200](#)

CLEAN DRIVE [212](#)

DEFINE DEVCLASS

3592 [102](#)

классы устройств LTO [99](#)

DEFINE DRIVE [97](#)

DEFINE LIBRARY [96](#)

UPDATE DRIVE [207](#), [208](#)

UPDATE LIBVOLUME [200](#)

UPDATE VOLUME [196](#)

VALIDATE LANFREE [126](#)

конфигурация

изменение [168](#)

клиенты [121](#)

конфигурация хранения

планирование [8](#)

конфигурирование

интервал времени для регистрации томов [134](#)

режим библиотеки [79](#)

совместно используемая библиотека (shared library) [105](#)

конфигурирование библиотек

SCSI [94](#)

копирование набора хранения на ленту [71](#), [77](#)

Л

лента

емкость [131](#)

лента (продолжение)

настройка периода задержки размонтирования [134](#)

ротация [196](#)

совместимость между накопителями [216](#)

формат записи [132](#)

ленточные накопители [2](#)

ленточный накопитель 3590

определение класса устройств [23](#)

ленточный накопитель, замена [216](#)

лицензирование эффективных единиц процессора (Processor Value Unit, PVU) [164](#)

лицензия на продукт

регистрировать (register) [61](#)

М

масштабирование емкости [103](#)

менеджер аварийного восстановления [67–69](#), [225](#), [227](#), [229](#), [230](#)

менеджер библиотеки, совместно используемая

библиотека [18](#), [108](#)

метка

автоматическая маркировка в библиотеках SCSI [190](#)

перезапись существующих меток [189](#), [190](#)

примеры томов [189](#)

проверка носителей [193](#)

пулы хранения с последовательным доступом [188](#)

регистрация [193](#)

считыватель штрих-кода [193](#)

тома, использующие устройство библиотеки [189](#)

метка носителя

для ленты [189](#)

запись [189](#)

проверка [193](#)

метки магнитных лент

перезаписать [91](#)

многонаправленный ввод-вывод

конфигурирование для систем AIX [42](#)

конфигурирование для систем Linux [43](#)

конфигурирование для систем Windows [45](#)

мониторинг

ежедневный контрольный список [143](#)

задачи

ежедневный контрольный список [143](#)

периодический контрольный список [155](#)

периодический контрольный список [155](#)

цели [143](#)

монтирование

библиотека [132](#)

ограничение [133](#)

операции [205](#)

период ожидания [134](#)

срок хранения [134](#)

query [205](#)

Н

накопители и носители 3592

включение носителей WORM [138](#)

определение класса устройств [23](#)

очистка [213](#)

параметр DEVICETYPE [191](#)

смешение поколений накопителей [102](#)

- накопители и носители 3592 (*продолжение*)
 - шифрование данных [104](#), [129](#)
- накопитель
 - адрес элемента [97](#)
 - задать [97](#)
 - обнаружение изменений в SAN [136](#)
 - обновить [207](#), [208](#)
 - очистка [212](#), [215](#)
 - серийный номер [97](#)
- несовместимость носителя [163](#)
- новый ленточный накопитель [216](#)
- носители
 - ротация лент [196](#)
- носители и устройства LTO Ultrium
 - класс устройств, определение и обновление [99](#)
 - шифрование [101](#), [129](#)
 - WORM [137](#)
- носители DLT WORM [137](#)
- носители Sony WORM (AIT50 и AIT100) [137](#)

O

- Об этой публикации [vii](#)
- обновление
 - server [223](#)
- обновление ленточных устройств [216](#)
- обновление системы
 - prepare [224](#)
- обслуживание
 - определить расписание [62](#)
- ограничение
 - доступ пользователей [221](#)
- операции архивирования
 - задание правил [115](#)
 - планирование [119](#)
- операции резервного копирования
 - задание правил [115](#)
 - изменение области [118](#)
 - планирование [119](#)
- операционная система
 - защита [220](#)
 - установка в серверных системах AIX [35](#)
 - установка в серверных системах Linux [37](#)
 - установка в серверных системах Windows [41](#)
- определить
 - интервал времени для проверки тома [134](#)
- опции
 - задать для сервера [53](#)
- опция, серверная
 - NOPREEMPT [135](#)
- остановка
 - server [221](#)
- отключение
 - prepare [224](#)
- отработка восстановления [229](#)
- отчеты
 - электронная почта
 - конфигурирование [165](#)
- отчеты о состоянии
 - получить [165](#)
- очистка накопителя [212](#)

P

- параметр AUTOLABEL для ленточных томов [190](#)
- параметр DRIVEENCRYPTION
 - класс устройств 3592 [104](#)
 - класс устройства LTO [101](#)
- пароли
 - изменение [219](#)
 - сброс [169](#)
- перевести носитель [67–69](#)
- переместить данные [67](#)
- перемещение данных в режиме без сети (LAN-free data movement)
 - Описание [18](#), [20](#)
- перенос данных [2](#)
- перенос данных на накопителях [217](#)
- периодический контрольный список задач мониторинга [155](#)
- планирование решений
 - лента [1](#)
- подготовка к аварии [225](#)
- политики
 - задать [115](#)
 - просмотр [116](#)
 - редактирование [116](#)
- последовательный режим для библиотек [79](#)
- правила
 - задать
 - операции резервного копирования и архивирования [115](#)
 - просмотр [116](#)
 - редактирование [116](#)
- правила хранения данных
 - задать [61](#)
- приемник клиента (client acceptor)
 - конфигурирование [122](#)
 - остановка [168](#)
 - перезапуск [168](#)
- приоритетное прерывание обслуживания
 - доступ к тому [136](#)
 - точка монтирования (mount point) [135](#)
- проблемы
 - диагностика [143](#)
- проверка данных
 - защита логических блоков [208](#)
- проверка ошибок
 - очистка накопителя [215](#)
- программная
 - выбор [113](#)
- производительность
 - часто используемый том, улучшение при более длительной задержке размонтирования [134](#)
- произвольный режим для библиотек [79](#)
- промежуточный драйвер [80](#)
- пропускная способность сети [2](#)
- пространство хранения
 - высвобождение [174](#)
- процесс деактивации
 - резервные данные [174](#)
- процесс списания
 - клиентский узел [171](#)
- публикации [vii](#)
- пул, система хранения
 - 3592, специальные замечания для [102](#)

пул, система хранения (*продолжение*)
решение об использовании совместного
размещения [177](#)
LTO Ultrium, специальные замечания [99](#)
пути
задать [95](#)

Р

рабочая таблица планирования [8](#)
расписания
операции резервного копирования и архивирования
[119](#)
реализация
операции проверки [141](#)
регистрация
клиенты [120](#)
настройка интервала времени для тома [134](#)
том библиотеки [191](#), [193](#)
чистящий картридж [214](#)
режим (mode)
библиотека (произвольная или последовательная)
[79](#)
режим доступа 'недоступно'
помеченный параметром PERMANENT [205](#)
режим обслуживания
сервер запуска [221](#)
решение
расширение [112](#)
решение на лентах
планирование [1](#)

С

свободные тома [198](#)
связь между клиентом и сервером
конфигурирование [125](#)
сервер (server)
задать опции [53](#)
задать расписание обслуживания [62](#)
конфигурировать [52](#)
создать ID пользователя для [45](#)
серверный параметр
NOPREEMPT [135](#)
серверный параметр NOPREEMPT [135](#)
серверы
запуск в режиме обслуживания [222](#)
серийный номер
автоматическое обнаружение сервером [96](#), [97](#), [136](#)
для библиотеки [96](#), [97](#)
для накопителя [97](#)
сеть хранения данных (SAN)
доступ клиентов к устройствам [18](#), [20](#)
изменения устройств, обнаружение [136](#)
перемещение данных в режиме без сети (LAN-free
data movement) [18](#), [20](#)
роль агента хранения [18](#), [20](#)
совместное использование библиотеки серверами
[18](#), [105](#)
слот хранения библиотеки [195](#)
слоты хранения библиотеки [192](#)
смешанные типы устройств в библиотеке [21](#), [22](#), [99](#), [102](#)
совместно используемая библиотека SCSI [105](#)

Совместное использование библиотеки [19](#)
совместное размещение
включение пула хранения с последовательным
доступом [177](#)
влияния на операции [179](#)
выбор томов при включении функции [181](#)
изменение, влияние [184](#)
как сервер выбирает тома при отключении [183](#)
определение [177](#)
планирование [186](#)
разрешение [186](#)
решение об использовании совместного
размещения [177](#)
совместное размещение пулов длительного хранения
[185](#)
сообщения
для автоматизированных библиотек [205](#)
соответствие лицензии
проверка [164](#)
состояние системы
отслеживание [165](#)
специальные возможности [233](#)
считыватель штрих-кода
аудит томов в библиотеке [202](#)

Т

тип устройств
несколько в одной библиотеке [21](#), [22](#)
LTO [99](#)
тип, устройство
несколько в одной библиотеке [21](#), [22](#)
LTO [99](#)
том в дистанционном хранилище [68](#), [73](#)
том на площадке [69](#), [74](#)
том хранения
маркировка с последовательным доступом [188](#)
подготовка с последовательным доступом [188](#)
тома
аудит [202](#)
время задержки размонтирования [134](#)
доступ, управление [196](#)
замена [194](#)
извлечение [200](#)
инвентарный список автоматической библиотеки
[203](#)
обновить [200](#)
обслуживание перечня [196](#)
определение монтированных [205](#)
приоритетное прерывание доступа [136](#)
пулы хранения с последовательным доступом [188](#)
размонтировать [205](#)
регистрация новых томов в библиотеки [191](#)
удаление из библиотеки [200](#)
управление [199](#)
тома хранения [71](#), [73](#), [74](#), [77](#)
тома worm [139](#)
точка монтирования (mount point)
приоритетное прерывание обслуживания [135](#)
связь с ограничением на монтирование в классе
устройств [133](#)
требования к аппаратным средствам [3](#)
требования к лентам [2](#)
требования к паролям

требования к паролям (продолжение)

LDAP [219](#)

требования к программному обеспечению [7](#)

требования к системе

аппаратная [3](#)

У

удалить накопитель [216](#)

узлы клиентов

списание [171](#)

удаление из производства [171](#)

управление

администраторы [218](#)

полномочия [218](#)

уровни доступа [221](#)

управление защитой [55](#)

уровень полномочий [218](#)

установка операционной системы

серверные системы AIX [35](#)

серверные системы Linux [37](#)

серверные системы Windows [41](#)

установка IBM Spectrum Protect

Системы AIX [49](#)

Системы Linux [49](#)

Системы Windows [51](#)

установки

клиенты [121](#)

устранение ошибок

заблокированные клиентские узлы [169](#)

ошибки в клиентских операциях [167](#)

ошибки паролей [169](#)

ID администратора [169](#)

устройства

задать [95](#)

Устройства и носители WORM

накопители Oracle StorageTek T10000B [138](#)

накопители Oracle StorageTek T10000C [138](#)

накопители Oracle StorageTek T10000D [138](#)

обслуживание томов в библиотеке [199](#)

специальные замечания о носителях WORM [137](#)

DLT WORM [137](#)

IBM 3592 [137](#)

LTO WORM [137](#)

Quantum LTO3 [137](#)

Sony AIT50 и AIT100; [137](#)

VolSafe

замечания о носителях [137](#)

устройства хранения [98](#)

устройства SCSI [87](#)

устройства, подключенные к SAN Fibre Channel [89](#)

устройства, подключенные по Fibre Channel [87](#)

устройство

драйвер устройства zfc [91](#)

несколько типов в библиотеке [21](#), [22](#)

name [81](#)

устройство автоматизированной библиотеки

аудит [202](#)

замена ленточного накопителя [216](#)

изменение состояния тома [200](#)

маркировка томов [189](#)

перечень томов [203](#)

регистрация томов [191](#)

уведомление сервера о новых томах [191](#)

устройство автоматизированной библиотеки (продолжение)

удаление томов [200](#)

устройство хранения

замена ленточного накопителя [216](#)

сведения об устройстве [137](#)

требуемые определения IBM Spectrum Protect [23](#)

устройство чтения штрих-кода

маркировка томов в библиотеке [190](#)

регистрация томов в библиотеке [193](#)

устройство, класс

задать [98](#)

параметр FORMAT [132](#)

LTO [99](#)

Ф

файла плана восстановления. [225](#)

файловые системы

планирование [8](#)

подготовка, серверные системы AIX [46](#)

подготовка, серверные системы Linux [48](#)

подготовка, серверные системы Windows [49](#)

файлы RPM

установка для графического мастера [50](#)

физические недостатки [233](#)

фронтальное лицензирование мощности [164](#)

Х

хранение

планирование [14](#), [16](#)

хранение вне площадки [26](#)

хранение, пул

3592, специальные замечания для [102](#)

решение об использовании совместного

размещения [177](#)

LTO Ultrium, специальные замечания [99](#)

Ц

Центр знаний vii

Центр знаний IBM vii

Центр операций

защищенная связь [59](#)

конфигурировать [58](#)

Ч

чистый том (scratch volume) [201](#)

чистящий картридж

операции с [163](#), [215](#)

регистрация [214](#)

Ш

шифрование

опции [29](#)

параметр DRIVEENCRYPTION

3592 Generation 2 [104](#)

LTO-4 или новее [101](#)

способы [127](#), [129](#)

шифрование данных [127](#)

Э

электронное хранилище [26](#)

электронные отчеты

 конфигурирование [165](#)



Номер программы: 5725-W98
5725-W99
5725-X15