IBM Spectrum Protect
для Linux
8.1.12

Руководство по установке

Примечание:

Прежде чем использовать эту информацию и описываемый в ней продукт, прочтите информацию в разделе “Замечания” на стр. 217.

Замечание по изданию

Данное издание относится к версии 8, выпуск 1, модификация 12 IBM Spectrum Protect (номера продукта 5725-W98, 5725-W99, 5725-X15), и ко всем последующим выпускам и модификациям, пока в новых изданиях не будет указано иное.

Содержание

Об этой публикации

Эта публикация содержит инструкции по установке и конфигурированию сервера IBM Spectrum Protect, языков сервера, лицензии, драйвера.

В эту публикацию также включены инструкции по установке компонента Центр операций.

Для кого предназначено это руководство

Эта публикация предназначена для системных администраторов, которые устанавливают, конфигурируют или обновляют сервер IBM Spectrum Protect или Центр операций.

Устанавливаемые компоненты

Сервер IBM Spectrum Protect и лицензии являются обязательными компонентами.

Эти компоненты содержатся в нескольких разных пакетах установки.

Таблица 1. Устанавливаемые компоненты IBM Spectrum Protect

компонент IBM Spectrum Protect	**Описание**	**Дополнительная информация**
Сервер (обязательно)	Содержит базу данных, Global Security Kit (GSKit), IBM® Java™ Runtime Environment (JRE) и утилиты, которые помогут вам сконфигурировать сервер и управлять им.	“Установка IBM Spectrum Protect при помощи мастера установки” на стр. 86
Пакет поддержки национального языка (необязательно)	Каждый пакет поддержки национального языка (по одному для каждого языка) содержит информацию на соответствующем языке для сервера.	Смотрите раздел “Установка языковых пакетов сервера” на стр. 89.
Лицензии (обязательно)	Обеспечивают поддержку всех лицензированных функций. После установки этого пакета необходимо зарегистрировать приобретенные лицензии.	Используйте команду **REGISTER LICENSE**.
Устройства (необязательно)	Расширяет возможности по управлению носителями.	Список устройств, поддерживаемых этим драйвером, смотрите по адресу: IBM Support Portal.

Таблица 1. Устанавливаемые компоненты IBM Spectrum Protect (продолжение)		
компонент IBM Spectrum Protect	**Описание**	**Дополнительная информация**
Агент хранения (необязательно)	Устанавливает компонент, который дает клиентским системам возможность непосредственно записывать данные на устройства хранения или непосредственно читать данные с устройств хранения, подключенных к сети хранения данных (Storage Area Network - SAN). **Напоминание:** IBM Spectrum Protect for Storage Area Networks - это отдельно лицензируемый продукт.	Дополнительные сведения об агентах хранения смотрите в разделе Tivoli Storage Manager for Storage Area Networks (V7.1.1).
Центр операций (необязательно)	Устанавливает Центр операций - это Web-интерфейс для управления средой хранения.	Смотрите раздел Часть 2, “Установка и обновление Центра операций”, на стр. 135.

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 смотрите в разделе Что нового.

Если в документации внесены изменения, они обозначаются вертикальной чертой (|) в поле.

Часть 1. Установка и обновление сервера

Установка и обновление сервера IBM Spectrum Protect.

Глава 1. Планирование установки сервера

Установите программное обеспечение сервера на компьютере, который управляет устройствами хранения, а программное обеспечение клиента - на каждой рабочей станции, которая передает данные в управляемое сервером IBM Spectrum Protect пространство хранения.

Что нужно знать в первую очередь

Перед первой установкой IBM Spectrum Protect необходимо собрать все сведения об используемых операционных системах, устройствах хранения данных, протоколах связи и системных конфигурациях.

Выпуски пакетов сервисного обслуживания сервера, программное обеспечение клиента и публикации есть по адресу: IBM Support Portal.

Ограничение: Сервер IBM Spectrum Protect можно установить и запустить в системе, в которой уже установлен продукт IBM Db2, невзирая на то, был ли продукт Db2 установлен независимо, или как часть какого-то другого приложения (с некоторыми ограничениями).

Дополнительные сведения смотрите в разделе “Совместимость сервера IBM Spectrum Protect с другими продуктами IBM Db2 в системе” на стр. 59.

Опытные администраторы Db2 могут выполнять сложные запросы SQL и использовать инструменты Db2 для мониторинга базы данных. Однако не используйте инструменты Db2, чтобы изменить параметры конфигурации Db2, заранее заданные продуктом IBM Spectrum Protect, и не изменяйте среду Db2 для IBM Spectrum Protect никакими другими способами, например с помощью других продуктов. Макрокоманда Сервер собран и подвергнут расширенному тестированию с использованием языка определений данных (Data Definition Language - DDL) и конфигурации базы данных, которые внедряет сервер.

Внимание: Не изменяйте программу Db2, устанавливаемую вместе с пакетами установки и пакетами исправлений IBM Spectrum Protect. Не устанавливайте другую версию, выпуск или пакет исправлений и не производите обновление до другой версии, выпуска или пакета исправлений программы Db2, так как это может привести к повреждению базы данных.

Что следует знать о защите перед установкой или обновлением сервера

Ознакомьтесь с информацией об улучшенных функциях защиты на сервере IBM Spectrum Protect и требованиях, предъявляемых к обновлению среды.

Перед началом работы

Начиная с версии 8.1.2, усовершенствования были добавлены в IBM Spectrum Protect, они обеспечивают более строгие параметры защиты. Прежде чем устанавливать или обновлять IBM Spectrum Protect, выполните следующие действия:

- Ознакомьтесь с информацией в разделе Защита в теме *Что нового* на сайте IBM Knowledge Center, чтобы узнать об обновлениях защиты в каждой версии.
- Если в вашей среде установлены прежние версии сервера, узнайте об ограничениях и известных проблемах в техническом замечании 562939. Чтобы устранить эти ограничения и воспользоваться новейшими мерами защиты, запланируйте обновление всех серверов IBM Spectrum Protect и клиентов резервного копирования и архивирования в вашей среде до новейшей версии.

Усовершенствования защиты

В версии V8.1.2 добавлены следующие усовершенствования защиты:

Протокол защиты, в котором используется протокол Transport Layer Security (TLS)

В программе IBM Spectrum Protect V8.1.2 и новее применяется улучшенный протокол защиты, использующий Transport Layer Security (TLS) 1.2 или новее для аутентификации сервера, агента хранения и клиентов резервного копирования и архивирования.

Начиная с IBM Spectrum Protect V8.1.11, можно включить протокол TLS 1.3 для защиты соединений между серверами, клиентами и агентами хранения. Чтобы использовать TLS 1.3, обе стороны в сеансе связи должны использовать TLS 1.3. Если любая из сторон использует TLS 1.2, по умолчанию обе стороны используют TLS 1.2.

Автоматическое конфигурирование SSL и распространение сертификатов

Серверы, агенты хранения и клиенты, использующие программное обеспечение версии 8.1.2 или новее, автоматически конфигурируются для аутентификации друг с другом с использованием TLS.

С помощью нового протокола у каждого сервера, агента хранения и клиента есть уникальный самоподписанный сертификат, который используется для аутентификации и разрешения соединений TLS. Самоподписанные сертификаты IBM Spectrum Protect обеспечивают защищенную аутентификацию между объектами, обеспечивают надежное шифрование для передачи данных и автоматически распространяют открытые ключи на клиентские узлы. Сертификаты автоматически передаются всем клиентам, агентам хранения и серверам, которые используют программное обеспечение версии 8.1.2 или новее. Вам не нужно вручную конфигурировать TLS или вручную устанавливать сертификаты для каждого клиента. Новые усовершенствования TLS не требуют изменений опций, и сертификаты передаются на клиенты автоматически при первом соединении, если только вы не используете один ID администратора для доступа к нескольким системам.

По умолчанию самоподписанные сертификаты распространяются, но при необходимости можно использовать другие конфигурации, такие как сертификаты, подписанные сертификатором. Дополнительную информацию об использовании сертификатов смотрите в разделе *Связь SSL и TLS* на сайте IBM Knowledge Center.

Сочетание протоколов TCP/IP и TLS для защищенной связи и минимального влияния на производительность

В предыдущих версиях программного обеспечения IBM Spectrum Protect нужно было выбрать TLS или TCP/IP, чтобы зашифровать все сообщения. Новый протокол защиты использует комбинацию TCP/IP и TLS для обеспечения защиты связи между серверами, клиентами и агентами хранения. По умолчанию, TLS используется только для шифрования аутентификации и метаданных, а протокол TCP/IP - для передачи данных. Поскольку шифрование TLS в первую очередь применяется только для аутентификации, то производительность операций резервного копирования и восстановления не влияет на производительность.

Необязательно: можно использовать TLS для шифрования передачи данных с помощью опции клиента **SSL** для связи клиент-сервер и параметра **SSL** в команде **UPDATE SERVER** для связи между сервером и сервером.

Обратная совместимость упрощает планирование обновлений в пакетах

Усовершенствованные версии серверов IBM Spectrum Protect и клиентов могут продолжать соединяться с более старыми версиями, если для параметра **SESSIONSECURITY** задано значение TRANSITIONAL.

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, продолжат 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, для которых используются разные версии, не прерывается. Однако вы не будете пользоваться преимуществами усовершенствования защиты, пока не будут обновлены и клиенты, и серверы.

Обеспечение строгого режима защиты с помощью параметра SESSIONSECURITY

Чтобы использовать новый протокол защиты, сервер, клиентский узел или объекты администратора должны использовать программное обеспечение IBM Spectrum Protect, которое поддерживает параметр **SESSIONSECURITY**. Защита сеанса - это уровень защиты, который используется для взаимодействий между узлами-клиентами IBM Spectrum Protect, клиентами администрирования и серверами. Для этого параметра можно задать следующие значения:

STRICT
Обеспечение высшего уровня защиты для связи между серверами IBM Spectrum Protect, узлами и администраторами, на сегодня это TLS 1.2.

TRANSITIONAL
Указывает, что существующий протокол связи (например, TCP/IP) используется до тех пор, пока вы не обновите программное обеспечение IBM Spectrum Protect до версии V8.1.2 или новее. 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.

Если задан параметр **SESSIONSECURITY=TRANSITIONAL** и сервер, узел или администратор никогда не соответствовал требованиям для значения STRICT, то сервер, узел или администратор продолжит проходить аутентификацию, используя значение TRANSITIONAL. Однако после того, как сервер, узел или администратор будут отвечать требованиям, предъявляемым к значению STRICT, значение параметра **SESSIONSECURITY** автоматически изменяется с помощью команды TRANSITIONAL на STRICT. После этого сервер, узел или администратор больше не сможет проходить аутентификацию, используя версию клиента или протокол SSL/TLS, не отвечающие требованиям для STRICT.

Ограничение: После того, как администратор успешно аутентифицируется на сервере с использованием программного обеспечения IBM Spectrum Protect V8.1.2 или более новой версии, или Tivoli Storage Manager V7.1.8 или более новой версии, администратор больше не сможет пройти аутентификацию на том же сервере, используя версии клиента или сервера более ранней версии, чем V8.1.2 или V7.1.8. Это ограничение относится также к серверу назначения при использовании таких функций, как маршрутизация команд, экспорт с сервера на сервер, аутентификация которого выполняется на сервере назначения IBM Spectrum Protect как администратор с другого сервера, подключения к администратору с помощью Центра операций и соединений из клиента командной строки администрирования.

В случае клиентских и административных сеансов, в сеансах выполнения команд администрирования может произойти сбой, если только администратор не получит сертификаты всех серверов, с которыми будет соединяться ID администратора. 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:

- 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.
- 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.

Перед выполнением обновления

Прежде чем обновлять сервер, ознакомьтесь с рекомендациями в следующей таблице контрольных проверок.

Таблица 2. Контрольный список планирования

Рекоиендация	**Описание**
Создайте резервные копии следующих файлов сервера: • Базы данных ключей (cert.kdb и dsmkeydb.kdb) • Файлы накопления (cert.sth и dsmkeydb.sth)	Начиная с IBM Spectrum Protect версии 8.1.2, главный ключ шифрования автоматически создается при запуске сервера, если главный ключ шифрования не существовал ранее. Главный ключ шифрования хранится в базе данных ключей, dsmkeydb.kdb. Сертификаты сервера по-прежнему хранятся в базе данных ключей cert.kdb и доступны для файла накопления cert.sth. Вы должны защитить обе базы данных ключей (cert.kdb и dsmkeydb.kdb) и файлы накопления паролей (cert.sth и dsmkeydb.sth), которые обеспечивают доступ к каждой из баз данных ключей. По умолчанию команда **BACKUP DB** защищает главный ключ шифрования таким же образом, как и журнал томов и файлы devconfig. Чтобы восстановить базу данных, вы должны запомнить пароль резервной копии базы данных. Файл `dsmserv.pwd` сервера IBM Spectrum Protect, который использовался для хранения главного ключа шифрования в предыдущих выпусках, больше не используется.
Тщательно запланируйте обновление для ID администраторов	Укажите все системы, которые используют учетные записи администратора, чтобы войти в систему в целях администрирования. После успешной аутентификации в версии 8.1.2 или более новой версии, администраторы не могут выполнять идентификацию в более ранних версиях программного обеспечения IBM Spectrum Protect на одном и том же сервере. Если для регистрации в нескольких системах используется один ID администратора, то запланируйте обновить все эти системы с помощью программного обеспечения версии 8.1.2 или новее, чтобы убедиться, что сертификат установлен во всех системах, где он входит в систему. **Совет:** Если параметр **SESSIONSECURITY** обновлен для всех ваших ID администраторов, так чтобы для него было задано значение STRICT, ваш доступ к серверу не заблокируют. Можно вручную импортировать открытый сертификат сервера в клиент, с которого вы выполняете команду **dsmadmc**.

Таблица 2. Контрольный список планирования (продолжение)

Рекоиендация	Описание
Если вы используете TLS с предыдущими версиями клиента, где используется сертификат "TSM Server SelfSigned Key" (cert.arm), то обновите клиенты до версии V8.1.4 или новее.	В выпусках до V7.1.8 сертификатом по умолчанию был сертификат "TSM Server SelfSigned Key" с подписью MD5, который не поддерживал протокол TLS 1.2 или новее, необходимый по умолчанию для клиентов V8.1.2 или новее и Центра операций. Чтобы устранить эту проблему, выполните одно из следующих действий: • Обновите сервер до V8.1.4 или новее. Начиная с V8.1.4, серверы, которые используют сертификат с подписью MD5, как сертификат по умолчанию, автоматически обновляются для использования сертификата по умолчанию с подписью SHA и меткой "TSM Server SelfSigned SHA Key". Копия нового сертификата по умолчанию хранится в файле `cert256.arm`, находящемся в каталоге экземпляра сервера. **Совет:** Перед обновлением сервера для использования нового сертификата по умолчанию с сигнатурой SHA распространите файл `cert256.arm` на клиенты, чтобы избежать ошибок резервного копирования клиентов. Каждый клиент должен получить и импортировать новый сертификат, прежде чем он сможет подключиться к серверу, использующему новый сертификат SHA по умолчанию. Предыдущие сертификаты удалять предыдущие сертификаты не требуется. • Чтобы вручную обновить сертификат по умолчанию, следуйте инструкциям в техническом замечании 562939.

Что делать дальше

- Чтобы установить или обновить сервер IBM Spectrum Protect, следуйте процедуре в разделе “Применение обновлений защиты” на стр. 7.
- Информацию об устранении неполадок связи, связанных с обновлениями защиты, смотрите в разделе “Устранение неполадок защиты” на стр. 14.
- Ответы на часто задаваемые вопросы (FAQ) смотрите в документе FAQ - Security updates in IBM Spectrum Protect (Часто задаваемые вопросы - обновления защиты в IBM Spectrum Protect).
- Информацию об использовании веб-клиента резервного копирования и архивирования IBM Spectrum Protect в новой среде защиты смотрите в техническом замечании 728037.

Применение обновлений защиты

Примените обновления защиты, которые поставляются с новыми выпусками IBM Spectrum Protect.

Прежде чем начать

Учтите следующую информацию:

- Подробную информацию об обновлениях защиты, поставляемых вместе с выпуском, смотрите в разделе *Что нового* на сайте IBM Knowledge Center.
- Просмотрите раздел “Что следует знать о защите перед установкой или обновлением сервера” на стр. 3, чтобы получить информацию об обновлениях и всех ограничениях, которые можно применить.
- Чтобы определить, в каком порядке обновлять серверы и клиенты в вашей среде, ответьте на следующие вопросы:

Таблица 3. Вопросы для рассмотрения перед обновлением

Вопрос	**Рекомендации**
Какова роль сервера в конфигурации?	В общем случае, сначала можно обновить серверы IBM Spectrum Protect в вашей среде, а затем обновить клиенты резервного копирования и архивирования. Однако при определенных обстоятельствах, например, если вы используете функции маршрутизации команд, сервер может выполнять функции клиента в вашей конфигурации. В этом случае, чтобы предотвратить проблемы связи, рекомендуется сначала обновить клиенты. Информацию о различных сценариях смотрите в разделе Сценарии обновления.

Таблица 3. Вопросы для рассмотрения перед обновлением (продолжение)

Вопрос	Рекомендации
Какие системы используются для аутентификации администратора?	Для учетных записей администратора последовательность, в которой выполняется обновление, важна для предотвращения проблем аутентификации. – Клиенты в нескольких системах, которые могут входить в систему с использованием одного и того же ID (ID узла или администратора), должны обновляться одновременно. Сертификаты сервера передаются на клиенты автоматически при первом соединении. – Перед обновлением сервера рассмотрите все конечные точки, которые администратор использует для подключения в административных целях. Если для доступа к нескольким системам применяется один административный ID, то убедитесь, что сертификат сервера установлен в каждой системе. – После того, как ID администратора успешно аутентифицируется на сервере с использованием программного обеспечения IBM Spectrum Protect V8.1.2 или более новой версии, или Tivoli Storage Manager 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. Это также относится и к серверу назначения, когда вы аутентифицируетесь на этом сервере назначения IBM Spectrum Protect как администратор с другого сервера. Например, это так, если вы используете следующие функции: - Маршрутизации команд - Экспорта с одного сервера на другой - Подключение из клиента администрирования в Центре операций

Таблица 3. Вопросы для рассмотрения перед обновлением (продолжение)

Вопрос	**Рекомендации**
В какой последовательности надо обновлять мои системы?	– **Если вы обновляете серверы прежде обновления клиентских узлов:** - Сначала обновите хаб-сервер, а затем - все подчиненные серверы. - При обновлении сервера до версии V8.1.2 или новее узлы и администраторы, использующие более раннюю версию программного обеспечения, могут продолжать взаимодействовать с новым сервером с использованием существующего протокола связи. Параметр **SESSIONSECURITY** имеет значение TRANSITIONAL, и если сервер, узел или администратор никогда не удовлетворяет требованиям для значения STRICT, то сервер, узел или администратор продолжает идентификацию с помощью значения TRANSITIONAL. Однако, как только сервер, узел или администратор отвечает требованиям, предъявляемым к значению STRICT, значение параметра **SESSIONSECURITY** автоматически изменяется с помощью команды TRANSITIONAL на STRICT. – **Если вы обновляете клиентские узлы прежде обновления серверов:** - Сначала обновите клиенты администрирования, а затем обновите клиенты, не связанные с административными клиентами. Клиенты более поздних выпусков продолжают обмениваться информацией с серверами более ранних уровней. **Важное замечание:** Если вы обновляете один из клиентов администрирования в вашей среде, то все остальные клиенты, использующие тот же ID, что и обновленный клиент, надо обновить одновременно. - Обновление всех клиентов, не являющихся клиентами, в одно и то же время не требуется, если только несколько клиентов не используют один и тот же ID для входа в систему. Затем все другие клиенты, которые используют тот же самый ID как обновленный клиент, должны быть модернизированы в то же время, и сертификат сервера должен быть установлен на каждой системе.

Об этой задаче

Если в вашей среде есть клиенты резервного копирования и архивирования IBM Spectrum Protect или серверы IBM Spectrum Protect более ранних версий, чем V7.1.8 или V8.1.2, вам может потребоваться настроить конфигурацию, чтобы обеспечить связь между серверами и клиентами без прерывания работы. Выполните описанную в этом разделе процедуру по умолчанию для установки или обновления среды.

Посмотрите в разделе Сценарии обновления другие примеры сценариев, которые могут быть применены к вашей среде.

Совет: Чтобы воспользоваться новейшими усовершенствованиями защиты, запланируйте обновление всех серверов IBM Spectrum Protect и клиентов резервного копирования и архивирования в среде до последнего уровня выпуска.

Процедура

1. Установите или обновите серверы IBM Spectrum Protect в среде. Дополнительные сведения смотрите в разделе *Установка и обновление сервера* на сайте IBM Knowledge Center.
   a) Обновите Центр операций и хаб-сервер. Дополнительную информацию смотрите в разделе Часть 2, “Установка и обновление Центра операций”, на стр. 135.
   b) Обновите подчиненные серверы.
   c) Настройка или проверка связи между серверами. Дополнительные сведения смотрите в следующих разделах:
      - Команда *UPDATE SERVER* в IBM Knowledge Center.
      - Раздел *Конфигурирование связи SSL между хаб-сервером и подчиненным сервером* в IBM Knowledge Center.
      - Раздел *Конфигурирование сервера для соединения с другим сервером при помощи SSL* в IBM Knowledge Center.

      Совет:

      - Начиная с версии IBM Spectrum Protect V8.1.2 и Tivoli Storage Manager V7.1.8, параметр **SSL** использует SSL для шифрования соединения с указанным сервером, даже если для параметра **SSL** задано значение NO.
      - Начиная с версии 8.1.4, сертификаты конфигурируются автоматически между агентами хранения, клиентами библиотеки и серверами библиотечного менеджера. Обмен сертификатами выполняется в первый раз, когда соединение между серверами устанавливается на сервере с повышенной защитой.
2. Установите или обновите административные клиенты. Дополнительную информацию смотрите в разделе *Установка и конфигурирование клиентов* в IBM Knowledge Center.
3. Включите защиту соединений между всеми системами, которые администраторы используют для входа в систему в административных целях.
   - Убедитесь, что программное обеспечение IBM Spectrum Protect, которое используется учетной записью администратора для входа в систему, обновлено до версии V8.1.2 или новее.
   - Если ID администратора входит в состав нескольких систем, то убедитесь, что сертификат сервера установлен в каждой системе.
4. Установите или обновите неадминистративные клиенты. Дополнительную информацию смотрите в разделе *Установка и конфигурирование клиентов* в IBM Knowledge Center.

   Напоминание: Неадминистративных клиентов можно обновлять синфазно. Вы можете продолжать соединяться с серверами более поздних уровней выпусков с клиентов более ранних выпусков, вводя команду **UPDATE NODE** и задавая для параметра **SESSIONSECURITY** значение TRANSITIONAL для каждого узла.

```
update node имя_узла sessionsecurity=transitional
```

Дальнейшие действия

К вашей среде могут применяться другие сценарии обновления. В следующей таблице приведены примеры сценариев обновления.

Таблица 4. Сценарии обновления

Сценарий	Замечания	Рекомендуемый подход к обновлению
Для маршрутизации команд на один или несколько серверов я использую функции маршрутизации команд администрирования. Я хочу подключиться к серверу IBM Spectrum Protect более ранней версии, чем V8.1.2.	• С помощью маршрутизации команд сервер может выполнять функции клиента администрирования. • Для маршрутизации команд используется идентификатор и пароль администратора, который ввел команду. • Если для доступа к нескольким системам применяется один административный ID, то убедитесь, что сертификат сервера установлен в каждой системе.	• Сначала обновите административный клиент. **Важное замечание:** Клиенты в нескольких системах, которые могут входить в систему с использованием одного и того же ID узла или администратора, должны обновляться одновременно. • На каждом сервере, на который выполняется маршрутизация команд, убедитесь, что сконфигурированы следующие данные: – Один и тот же ID администратора и пароль – Необходимые полномочия администратора на каждом сервере – Установлены необходимые сертификаты • Обновите серверы, используемые учетной записью администратора для входа в V8.1.2 или более новой версии.

Таблица 4. Сценарии обновления (продолжение)

Сценарий	Замечания	Рекомендуемый подход к обновлению
Версия моего административного клиента - это последняя версия выпуска, и я использую тот же ID администратора для аутентификации в разных системах с помощью команды **dsmadmc**. Я успешно аутентифицирован на сервере IBM Spectrum Protect в моей среде, работающей в последней версии. Теперь я хочу пройти аутентификацию на сервере более ранней версии, чем V8.1.2.	• После того как администратор пройдет аутентификацию на сервере IBM Spectrum Protect V8.1.2 или новее, используя клиент версии V8.1.2 или новее, административный ID сможет проходить аутентификацию только на клиентах или серверах, использующих V8.1.2 или новее. • Если для доступа к нескольким системам применяется один административный ID, то запланируйте обновить все системы с помощью версии 8.1.2 или более новой версии, чтобы убедиться, что сертификат сервера установлен во всех системах, где администратор входит в систему.	• Убедитесь, что все программное обеспечение IBM Spectrum Protect, которое администраторы используют для входа в систему, обновлено до версии V8.1.2 или новее. Предпочтительное действие - обновить все серверы в вашей среде до последней версии. • 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.
Сервер IBM Spectrum Protect уже обновлен до уровня последнего выпуска. У меня есть административный клиент на уровне выпуска V8.1.0, и я хочу соединиться с сервером из Центра операций.	• Если вы обновляете один из клиентов администрирования в вашей среде, то все остальные клиенты, использующие тот же ID, что и обновленный клиент, надо обновить одновременно. • Чтобы использовать ID администратора в конфигурации с несколькими серверами, этот ID должен быть зарегистрирован на хаб-сервере и на серверах с одним и тем же паролем, уровнем полномочий и требуемыми сертификатами.	• Убедитесь в том, что на каждом сервере задана следующая информация: – Один и тот же ID администратора и пароль – Необходимые полномочия администратора на каждом сервере – Необходимые сертификаты • Обновите неадминистративные клиенты поэтапно.
Я использую репликацию узла для защиты своих данных.	• Контрольный сигнал репликации инициирует обмен сертификатами при установлении первого соединения одного сервера с другим после обновления сервера.	• Перед обновлением клиентов необходимо обновить серверы; выполните процедуру по умолчанию.

Таблица 4. Сценарии обновления (продолжение)

Сценарий	Замечания	Рекомендуемый подход к обновлению
Я хочу обновить клиенты резервного копирования и архивирования, прежде чем обновлять мои серверы.	• После обновления сервера до V8.1.2 или новее узлы и администраторы, использующие более ранние версии программы, продолжат взаимодействовать с сервером, используя значение TRANSITIONAL, пока объект будет соответствовать требованиям для значения STRICT. • Связь между серверами и клиентами не будет прервана.	• Если вы обновляете клиенты до обновления серверов, то сначала обновите клиенты администрирования, а затем обновите клиенты, не связанные с административными клиентами. Клиенты более поздних выпусков продолжают обмениваться информацией с серверами более ранних уровней.

Устранение неполадок защиты

Устраните неполадки, которые могут возникнуть после обновления IBM Spectrum Protect.

Симптом	Разрешение
Учетная запись администратора не может войти в систему, которая использует программное обеспечение более ранней версии, чем V8.1.2.	После того, как администратор успешно аутентифицируется на сервере с помощью IBM Spectrum Protect версии 8.1.2 или более новой версии, этот администратор больше не сможет пройти аутентификацию на сервере, который использует версии клиента или сервера более ранней версии, чем V8.1.2. Это ограничение относится также к серверу назначения при использовании таких функций, как маршрутизация команд, экспорт с сервера на сервер, аутентификация которого выполняется на сервере назначения IBM Spectrum Protect как администратор с другого сервера, подключения к администратору, которые используют Центр операций, и соединения из клиента командной строки администрирования. Чтобы устранить проблемы аутентификации для администраторов, выполните следующие действия: 1. Укажите все системы, в которых администраторы могут входить в систему и использовать административный ID для входа в систему. Обновите системное программное обеспечение до версии IBM Spectrum Protect V8.1.2 или более новой и убедитесь, что сертификат сервера установлен в каждой системе. 2. Задайте значение параметра **SESSIONSECURITY** для администратора в TRANSITIONAL, для чего введите команду `update admin` *`имя_администратора`* `sessionsecurity=transitional` 3. Повторите попытку соединения с администратором. **Совет:** 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.
Не удалось выполнить рассылку сертификатов для узла, администратора или сервера.	У узла, администратора или сервера, использующего программное обеспечение версии 8.1.2 или новее, есть значение **SESSIONSECURITY** STRICT, но нужно сбросить значение в TRANSITIONAL, чтобы повторить распространение сертификата.

Симптом	Разрешение

	При использовании нового протокола автоматическая передача публичного сертификата сервера выполняется только при первом соединении с сервером с повышенной защитой. После первого соединения значение параметра **SESSIONSECURITY** для узла изменится с TRANSITIONAL на STRICT. Вы можете временно обновить узел, администратор или сервер до состояния TRANSITIONAL, чтобы разрешить другую автоматическую передачу сертификата. При необходимости в TRANSITIONAL следующее соединение автоматически передает сертификат, если он необходим, и сбрасывает значение параметра **SESSIONSECURITY** в STRICT.
	
	Измените значение параметра **SESSIONSECURITY** на TRANSITIONAL, введя одну из следующих команд:
	
	• Для клиентских узлов выполните следующие действия:
	`update node` *`имя_узла`* `sessionsecurity=transitional`
	• Для администраторов введите:
	`update admin` *`имя_администратора`* `sessionsecurity=transitional`
	• Для серверов введите:
	`update server` *`имя_сервера`* `sessionsecurity=transitional`
	
	Другой способ: можно вручную передать и импортировать общий сертификат с помощью утилиты dsmcert, чтобы ввести следующие команды:
	
	`openssl s_client -connect tapsrv04:1500 -showcerts > tapsrv04.arm`
	
	`dsmcert -add -server tapsrv04 -file tapsrv04.arm`
	
	Если вы используете сертификаты, подписанные CA, то вы должны установить в каждой базе данных ключей клиента, сервера и агента хранения, который инициирует связь SSL, сертификатор (CA) и все CA-промежуточные сертификаты для каждого из них.

Обмен сертификатами между серверами IBM Spectrum Protect не был успешен.	При использовании нового протокола автоматическая передача публичного сертификата сервера выполняется только при первом соединении с сервером с повышенной защитой. После первого соединения значение параметра **SESSIONSECURITY** для сервера изменится с TRANSITIONAL на STRICT. Повторите обмен сертификатами между двумя серверами IBM Spectrum Protect. Информацию смотрите в разделе *.Повторная попытка обмена сертификатами между серверами*.
Обмен сертификатами между сервером IBM Spectrum Protect и клиентским узлом не был успешен.	При использовании нового протокола автоматическая передача публичного сертификата сервера выполняется только при первом соединении с сервером с повышенной защитой. После первого соединения значение параметра **SESSIONSECURITY** для узла изменится с TRANSITIONAL на STRICT. Чтобы повторить попытку обмена сертификатами между клиентами и серверами версии ниже V8.1.2, выполните следующие действия: 1. В случае существующих клиентов, сконфигурированных для использования SSL с сертификатом cert.arm, переконфигурируйте их так, чтобы они использовали сертификат `cert256.arm`. Инструкции смотрите в следующих разделах: *Конфигурирование агентов хранения, серверов, клиентов и Центра операций для соединения с сервером с использованием SSL* в IBM Knowledge Center.

Симптом	Разрешение

	2. Обновите сертификат по умолчанию, введя следующую команду из каталога экземпляра сервера:
	`gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed -label "TSM Server SelfSigned SHA Key"`
	3. Перезапустите сервер.
	В случае клиентов и серверов версии 8.1.2 и более новых версий сертификаты распространяются автоматически. Если происходит сбой связи между клиентами или серверами, выполните следующие действия, чтобы повторить попытку получения сертификата:
	1. Для узлов и администраторов задайте для параметра **SESSIONSECURITY** значение TRANSITIONAL, введя следующие команды для каждого узла или администратора, для которого вы хотите повторить попытку:
	`update node` *`имя_узла`* `sessionsecurity=transitional`
	`update admin` *`имя_администратора`* `sessionsecurity=transitional`
	Совет: 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:
	• 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 входит в систему из нескольких систем, то убедитесь, что сертификат сервера установлен в каждой системе до того, как учетная запись администратора будет использоваться для маршрутизации команд.
	• После того как администратор пройдет аутентификацию на сервере V8.1.2 или новее, используя клиент V8.1.2 или новее, администратор сможет проходить аутентификацию только на клиентах или серверах, использующих V8.1.2 или новее. 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.
	2. Для агентов хранения обновите значение параметра **STASESSIONSECURITY** в файле опций агента хранения `dsmsta.opt`, изменив значение STRICT на TRANSITIONAL.
	3. Перезапустите серверы. Изменения сертификата не будут действовать до тех пор, пока вы не перезапустите серверы или агенты хранения.
	4. Если вы по-прежнему не можете обмениваться сертификатами после выполнения шагов 1-4, то добавьте сертификаты вручную на серверы и агенты хранения и перезапустите их. Инструкции смотрите в следующих разделах: *Конфигурирование агентов хранения, серверов, клиентов и Центра операций для соединения с сервером с использованием SSL* в IBM Knowledge Center.

Вы хотите вручную распространить сертификаты на клиентские системы.	Администратор сервера IBM Spectrum Protect может автоматически внедрить клиент резервного копирования и архивирования, чтобы обновить рабочие станции, на которых уже установлен клиент резервного копирования и архивирования. Информацию смотрите в

Симптом	Разрешение
	разделе *Автоматическое внедрение клиента резервного копирования и архивирования* в IBM Knowledge Center. Чтобы вручную добавить сертификаты в клиенты, смотрите раздел *Конфигурирование связи между клиентом и сервером IBM Spectrum Protect с помощью Secure Sockets Layer* в IBM Knowledge Center.
Вы хотите сбросить сертификаты для сеансов клиент-клиент	Утилита dsmcert, которая устанавливается вместе с клиентом резервного копирования и архивирования IBM Spectrum Protect, используется для создания склада сертификатов для сертификатов сервера. Используйте утилиту dsmcert, чтобы удалить файлы и заново импортировать сертификаты.
Вы, как пользователь root, хотите позволить другим пользователям (без полномочий root) управлять своими файлами.	Агент TCA (trusted communications agent - агент доверенной связи), ранее используемый пользователями без полномочий root в V8.1.0, V7.1.6 и более ранних клиентах IBM Spectrum Protect, более не доступен. Пользователи root могут использовать следующие способы, чтобы позволить пользователям без полномочий root управлять их файлами: **Способ с обращением за помощью** При этом способе все операции резервного копирования и восстановления выполняет пользователь root. Пользователь без полномочий root должен обратиться к пользователю root и попросить выполнить резервное копирование или восстановление определенных файлов. **Способ уполномоченного пользователя** При использовании этого способа пользователю без полномочий root дается доступ для чтения и записи к складу паролей при помощи опции `passworddir`, которая указывает на положение паролей, доступное для чтения и записи пользователю без полномочий root. Этот способ позволяет пользователям без полномочий root выполнять резервное копирование и восстановление их собственных файлов, использовать шифрование и управлять своими паролями при помощи опции `passwordaccess generate`. Дополнительную информацию смотрите в разделе *Разрешение пользователям без полномочий root управлять своими данными* в IBM Knowledge Center . Если ни один из этих способов вам не подходит, надо использовать более ранние клиенты, включенные в TCA.
Вы хотите устранить проблемы совместимости GSKit.	Если несколько прикладных программ, использующих GSKit, установлены в одной системе, могут возникнуть проблемы совместимости. Чтобы устранить эти проблемы, ознакомьтесь со следующей информацией: • Для клиентов IBM Spectrum Protect смотрите Техническое замечание 2011742. • Для Db2 смотрите Техническое замечание 7050721. • Для сервера IBM Spectrum Protect смотрите Техническое замечание 2007298. • Для сервера и клиента IBM Spectrum Protect в одной и той же системе Windows смотрите Техническое замечание 7050721.

Дополнительную информацию об устранении неполадок, связанных с обновлениями защиты, смотрите в техническом замечании 2004844.

Повторная попытка обмена сертификатами между серверами

Если обмен сертификатами между серверами завершится неудачно, можно попытаться произвести другой обмен.

Процедура

1. Удалите сертификат из базы данных сервера партнера, введя на обоих серверах следующую команду:

   ```
   update server имя_сервера forcesync=yes
   ```

   Совет: Если после выполнения шагов в этой задаче и перезапуска серверов вы все еще получаете сообщения об ошибках для каждого сеанса взаимодействий сервера с сервером, возможно, что сервер использует неправильный сертификат. Если вы установите, что сервер пытается использовать неправильный сертификат, удалите сертификат из базы данных ключей, введя следующую команду:

   ```
   gsk8capicmd_64 -cert -delete -db cert.kdb -stashed -label имя_метки_сертификата
   ```

2. Удалите определение сервера, введя команду **DELETE SERVER** как для сервера, так и для сервера партнера. Если вы не можете удалить определение сервера, вы должны сконфигурировать сертификаты вручную. Инструкции по конфигурированию сертификатов вручную смотрите под заголовком *Конфигурирование агентов хранения, серверов, клиентов и Центра операций для соединения с сервером с использованием SSL* в разделе IBM Knowledge Center.
3. Чтобы повторно получить сертификат, задайте серверы перекрестно по отношению друг к другу и разрешите им обмен сертификатами, введя следующие команды на обоих серверах:

   ```
   set crossdefine on
   set serverhladdress hl-адрес
   set serverlladdress ll-адрес
   set serverpassword пароль
   ```

4. Введите следующую команду на одном из серверов, которые вы задаете перекрестным образом:

   ```
   define server имя_сервера crossdefine=yes ssl=yes
   ```

5. Повторите шаг 3 для всех других пар серверов версии 8.1.2 или новее.
6. Перезапустите серверы.
7. Чтобы убедиться, что обмен сертификатами произошел, введите следующую команду из каталога экземпляра каждого сервера, для которого вы хотите произвести проверку:

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

   Вывод примера:

   ```
   example.website.com:1542:0
   ```

   Совет: Если вы используете репликацию, при первом соединении после обновления сервера появятся контрольные сигналы репликации в течение, приблизительно, каждых 5 минут, и инициализируется обмен сертификатами. При этом соединении в журнале один раз появляются сообщения ANR8583E и ANR8599W перед проведением обмена сертификатами. Если вы не используете репликацию, то при первой инициализации сеанса сервера с сервером, кроме конфигурирования сервера, когда сервер не задан на обоих компьютерах.
8. Для серверов, которые заданы как виртуальный том, выполните следующие действия:
   a) Удалите сертификат партнера из базы данных сервера, введя на обоих серверах следующую команду:

```
update server имя_сервера forcesync=yes
```

b) Убедитесь, что один и тот же пароль используется в качестве значения пароля сервера в команде **DEFINE SERVER** на исходном сервере, в качестве значения пароля в команде **REGISTER NODE** на сервере виртуальных томов, также в качестве значения **SET SERVERPASSWORD** на сервере виртуальных томов. Если потребуется, обновите пароль, используя команды **UPDATE SERVER**, **UPDATE NODE** или **SET SERVERPASSWORD**, соответственно. Обмен сертификатами осуществляется после первой операции резервного копирования клиента с сервера виртуального тома на исходный сервер.

9. Если вам все еще не удается произвести обмен сертификатами между серверами, сделайте следующее:
   a) В определении сервера для каждого из взаимодействующих серверов убедитесь, что вы указали имя сервера, совпадающее с именем, заданным при вводе команды **SET SERVERNAME** на сервере партнера.
   b) Убедитесь, что в определениях серверов содержатся пароли, заданные с помощью команды **SET SERVERPASSWORD**. Пароли должны совпадать со значением, заданным с помощью команды **SET SERVERNAME** для сервера партнера.
   c) После выполнения шагов a и b снова введите следующую команду:

```
update server имя_сервера forcesync=yes
```

   d) Повторите шаги с 1 по 3.

Планирование для достижения оптимальной производительности

Прежде чем устанавливать сервер IBM Spectrum Protect, оцените характеристики и конфигурацию системы, чтобы убедиться, что сервер настроен для оптимальной производительности.

Об этой задаче

Оптимальная среда IBM Spectrum Protect настраивается с использованием IBM Spectrum Protect Blueprints.

Процедура

1. Ознакомьтесь с разделом “Что нужно знать в первую очередь” на стр. 3.
2. Прочтите каждый из следующих подразделов.

Планирование оборудования и операционной системы сервера

Используйте контрольный список, чтобы убедиться, что система, в которой установлен сервер, соответствует требованиям к конфигурации оборудования и программ.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Соответствуют ли операционная система и оборудование требованиям или превышают их? • Число и частота процессоров • Системная память • Поддерживаемый уровень операционной системы	Если вы используете минимально необходимый объем памяти, вы можете поддерживать минимальную рабочую нагрузку. Вы можете поэкспериментировать, добавляя больше системной памяти, чтобы определить, повышается ли производительность. Затем решите, хотите ли вы оставить системную память выделенной для сервера. Проверьте различные вариации памяти, используя весь ежедневный цикл рабочей нагрузки сервера. Если у вас в системе работает несколько серверов, прибавьте требования для каждого сервера, чтобы получить требования к системе.	Прочтите требования к операционной системе в техническом замечании 1243309. Кроме того, смотрите рекомендации в документе Задачи по настройке для операционной системы и других приложений. Дополнительную информацию о требованиях при использовании этих возможностей, смотрите в следующих разделах: • Контрольный список для дедупликации данных • Контрольный список по репликации узлов Дополнительную информацию о том, как подобрать размер для сервера и хранения, смотрите в документе IBM Spectrum Protect Blueprint.
Сконфигурированы ли диски для оптимальной производительности?	Объем настройки, которую нужно производить для разных дисковых систем, различается. Убедитесь, что задана соответствующая глубина очереди и другие опции дисковых систем.	Дополнительные сведения смотрите в следующих разделах: • "Планирование дисков базы данных сервера" • "Планирование для дисков журнала восстановления сервера" • "Планирование для пулов хранения на устройствах классов устройств DISK или FILE"

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Достаточно ли памяти на сервере?	Для более высоких рабочих нагрузок и таких дополнительных функций, как дедупликация данных и репликация узлов, требуется объем системной памяти, превышающий минимальный объем, указанный в документе с требованиями к системе. Для баз данных, не включенных для дедупликации данных, используйте следующие рекомендации по определению требований к системной памяти: • Для баз данных, объемом менее 500 ГБ, требуется 16 ГБ памяти. • Для баз данных, объемом от 500 ГБ до 1 ТБ, требуется 24 ГБ памяти. • Для баз данных, объемом от 1 ТБ до 1,5 ТБ, требуется 32 ГБ памяти. • Для баз данных, объем которых превышает 1,5 ТБ, требуется 40 ГБ памяти. Убедитесь, что вы выделили дополнительное пространство для активного и архивного журналов для обработки репликации.	Дополнительную информацию о требованиях при использовании этих возможностей, смотрите в следующих разделах: • Контрольный список для дедупликации данных • Контрольный список по репликации узлов • Требования к памяти

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Есть ли в системе достаточное число адаптеров шины хоста (host bus adapter, HBA) для обработки операций с данными, которые сервер IBM Spectrum Protect должен выполнять одновременно?	Определите, для каких операций требуется использовать HBA одновременно. Например, серверу нужно сохранять 1 ГБ/сек данных резервных копий и при этом также нужно производить перенастройку пула хранения, для выполнения чего требуется 0,5 ГБ/сек. HBA должны быть способны обрабатывать все эти данные с нужной скоростью.	Смотрите раздел Настройка емкости HBA.
Превышает ли ширина полосы пропускания сети запланированную максимальную пропускную способность для резервнных копий?	Полоса пропускания сети должна позволять системе выполнять такие операции, как резервное копирование, когда это разрешено или соответствует обязательствам на уровне услуг. Для репликации узлов полоса пропускания сети должна быть больше запланированной максимальной пропускной способности.	Дополнительные сведения смотрите в следующих разделах: • Настройка производительности сети • Контрольный список по репликации узлов

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Используете ли вы предпочтительную файловую систему для файлов сервера IBM Spectrum Protect?	Используйте файловую систему, обеспечивающую оптимальную производительность и доступность данных. Сервер использует прямой ввод-вывод для файловых систем, поддерживающих эту функцию. Использование прямого ввода-вывода может повысить пропускную способность и уменьшить степень использования процессора. Более подробную информацию о предпочтительной файловой системе для вашей операционной системы смотрите в документе Файловые системы, поддерживаемые сервером IBM Spectrum Protect.	Дополнительную информацию смотрите в разделе Конфигурирование операционной системы для производительности дисков.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Планируете ли вы сконфигурировать достаточное пространство подкачки?	Пространство подкачки (или свопинга) расширяет память, доступную для обработки. Если объем свободной RAM в системе мал, программы или данные, которые не используются, перемещаются из памяти в пространство подкачки. Это действие высвобождает память для других операций, например, операций базы данных. **Ограничение:** Не используйте пространство подкачки для добавления памяти в систему. Пространство подкачки предназначено только для ограниченного и временного расширения пространства. Если ваша система использует пространство подкачки, значит, системная память полна и её надо расширить. Используйте, как минимум, 32 ГБ пространства подкачки или 50% оперативной памяти в зависимости от того, какое значение будет больше.	
Собираетесь ли вы настроить параметры ядра после установки сервера?	Вы должны настроить параметры ядра.	Смотрите информацию о настройке параметров ядра: Linux®: Настройка параметров ядра для систем Linux

Планирование для дисков базы данных сервера

Используйте контрольный список, чтобы убедиться, что система, в которой установлен сервер, соответствует требованиям к конфигурации оборудования и программ.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Находится ли база данных на быстрых дисках с низкой латентностью?	Не используйте для базы данных IBM Spectrum Protect следующие накопители: • Nearline SAS (NL-SAS) • Serial Advanced Technology Attachment (SATA) • Parallel Advanced Technology Attachment (PATA) Не используйте внутренние диска, включенные по умолчанию в большинство аппаратных компонентов серверов. Твердотельные диски (solid-state disks, SSD) уровня предприятия с оптоволоконным интерфейсом или интерфейсом SAS предлагают наивысшую производительность. Если вы собираетесь использовать функции дедупликации данных в IBM Spectrum Protect, обратите внимание на производительность дисков в виде числа операций ввода-вывода в секунду (I/O operations per second, IOPS).	Дополнительную информацию смотрите в разделе Контрольный список для дедупликации данных.
Хранится ли база данных на дисках или LUN отдельно от дисков или LUN, используемых для активного журнала, архивного журнала и томов пула хранения?	Если отделить базу данных сервера от других серверных компонентов, это поможет сократить число конфликтов за одни и те же ресурсы среды различных операций, которые должны выполняться одновременно. **Совет:** База данных и архивный журнал могут совместно использовать массив, когда вы применяете технологию твердотельных накопителей (solid-state drive, SSD).	

Вопрос	**Задачи, характеристики, опции или параметры**	**Дополнительная информация**
Если вы используете RAID, знаете ли вы, как выбрать оптимальный уровень RAID для вашей системы? Задаете ли вы все LUN одного и того же размера и типа RAID?	Если системе нужно производить большое число операций записи, RAID 10 превосходит RAID 5. Однако для RAID 10 требуется больше дисков, чем для RAID 5 при одном и том же объеме используемого пространства хранения. Если в вашей дисковой системе используется RAID, задайте все ваши LUN с использованием одного и того же размера и типа RAID. Например, не смешивайте 4+1 RAID 5 с 4+2 RAID 6.	
Если доступна опция задать размер полосы или размер сегмента, планируете ли вы оптимизировать размер при конфигурировании дисковой системы?	Если вы можете задать размер полосы или размер сегмента, используйте в дисковых системах для базы данных размер, равный 64 КБ или 128 КБ.	Размер блока, используемого для базы данных, зависит от табличного пространства. Большинство таблиц используют блоки по 8 КБ, но некоторые используют блоки по 32 КБ.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Планируете ли вы создать хотя бы четыре каталога, которые также называются путями хранения, на четырех отдельных LUN для базы данных? Создайте по одному каталогу на отдельный массив в подсистеме. Если у вас менее трех массивов, создайте внутри массива отдельный том LUN.	При более высоких рабочих нагрузках и использовании некоторых функций требуется больше путей хранения, чем это соответствует минимальным требованиям. Такие операции сервера, как дедупликация данных, приводят к более высокому числу операций ввода-вывода в секунду (input/output operations per second, IOPS) для базы данных. Такие операции лучше выполняются, если у базы данных больше каталогов. В случае баз данных серверов, размер которых превышает 2 ТБ или которые, как ожидается, вырастут до этого размера, используйте восемь каталогов. При определении того, сколько путей хранения следует создать, рассмотрите запланированный рост системы. Сервер эффективнее использует высокое число путей хранения, если пути хранения присутствовали при первом создании сервера. Используйте переменную *DB2_PARALLEL_IO*, чтобы принудительно производить параллельный ввод-вывод в табличных пространствах, у которых один контейнер, или в табличных пространствах, контейнеры которых находятся более чем на одном физическом диске. Если вы не зададите переменную *DB2_PARALLEL_IO*, параллелизм ввода-вывода будет равен числу контейнеров, используемых табличным пространством. Например, если табличное пространство охватывает четыре контейнера, используемый уровень параллелизма ввода-вывода будет равен 4.	Дополнительные сведения смотрите в следующих разделах: • Контрольный список для дедупликации данных • Контрольный список по репликации узлов Справку относительно того, как предсказать рост, когда сервер производит дедупликацию данных, смотрите в техническом замечании 1596944. Последнюю информацию о размере базы данных, реорганизации базы данных и замечания относительно производительности для серверов IBM Spectrum Protect смотрите в техническом замечании 1683633. Информацию о настройке переменной *DB2_PARALLEL_IO* смотрите в документе Рекомендуемые параметры для переменных реестра IBM Db2.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Является ли размер всех каталогов для базы данных одинаковым?	Каталоги одного и того же размера обеспечивают одинаковую степень параллелизма для операций базы данных. Если размер одного или нескольких каталогов для базы данных меньше размера остальных каталогов, то потенциал оптимизированного предварительного извлечения снизится. Эта рекомендация также применима, если вам нужно добавить пути хранения после первоначального конфигурирования сервера.	
Собираетесь ли вы увеличить глубину очереди для LUN базы данных в системах AIX?	Глубина очереди по умолчанию часто оказывается слишком мала.	Смотрите раздел Конфигурирование систем AIX для производительности диска.

Планирование для дисков журнала восстановления сервера

Используйте контрольный список, чтобы убедиться, что система, в которой установлен сервер, соответствует требованиям к конфигурации оборудования и программ.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Хранятся ли активный журнал и архивный журнал на дисках или на LUN отдельно от дисков или LUN, используемых для базы данных и томов пула хранения?	Убедитесь, что диски, на которых вы размещаете активный журнал, не используются для других задач сервера или системы. Не помещайте активный журнал на диски, содержащие базу данных сервера, архивный журнал или такие системные файлы, как пространство подкачки или свопинга.	Если отделить базу данных сервера, активный журнал и архивный журнал, это поможет сократить число конфликтов за одни и те же ресурсы среды различных операций, которые должны выполняться одновременно.
Находятся ли журналы на дисках с энергонезависимым кэшем записи?	Энергонезависимый кэш записи позволяет как можно быстрее записывать данные в журналы. Более быстрые операции записи для журналов могут повысить производительность операций сервера.	

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Задаете ли вы для журналов размер, который адекватно поддерживает рабочую нагрузку?	Если вы не уверены относительно рабочей нагрузки, используйте самый большой возможный для вас размер. **Активный журнал** Максимальный размер - 512 ГБ, заданный с помощью опции сервера **ACTIVELOGSIZE**. Убедитесь, что у вас есть хотя бы 8 ГБ свободного пространства в файловой системе активного журнала после создания активных журналов фиксированного размера. **Архивный журнал** Размер архивного журнала ограничен размером файловой системы, в которой он находится, а не опцией сервера. Убедитесь, что размер архивного журнала, как минимум, равен размеру активного журнала.	• Подробную информацию о размерах журналов смотрите в информации о журнале восстановления в техническом замечании 400357. • Информацию о подборе размеров при использовании дедупликации данных смотрите в разделе Контрольный список для дедупликации данных.
Задаете ли вы архивный журнал передачи управления при отказе? Размещаете ли вы этот журнал на диске, являющемся отдельным по сравнению с диском архивного журнала?	Архивный журнал передачи управления при отказе предназначен для использования сервером в аварийных ситуациях, когда архивный журнал переполняется. Для архивного журнала передачи управления при отказе можно использовать более медленные диски.	Используйте опцию сервера **ARCHFAILOVERLOGDIRECTORY**, чтобы указать расположение архивного журнала передачи управления при отказе. Отслеживайте использование каталога для архивного журнала передачи управления при отказе. Если архивный журнал передачи управления при отказе должен использоваться сервером, пространство архивного журнала может оказаться недостаточным.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Если вы производите зеркальное отображение активного журнала, используете ли вы только один тип зеркального отображения?	Зеркальное отображение журнала можно производить, используя один из описанных ниже методов. Используйте для журнала только один тип зеркального отображения. • Используйте опцию **MIRRORLOGDIRECTORY**, которая доступна для сервера IBM Spectrum Protect, чтобы задать расположение зеркального отображения. • Используйте в AIX зеркальное отображение программ, например, Logical Volume Manager (LVM). • Используйте зеркальное отображение на оборудовании дисковых систем.	Если вы зеркально отображаете активный журнал, убедитесь, что у дисков для активного журнала и зеркальной копии одинаковая скорость и надежность. Дополнительную информацию смотрите в разделе Конфигурирование и настройка журнала восстановления.

Планирование для пулов хранения каталогов-контейнеров и пулов хранения облачных контейнеров

Проверьте, как настроены пулы хранения каталогов-контейнеров и облачных контейнеров, чтобы убедиться, что они обеспечивают оптимальную производительность.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Используете ли вы быстрое дисковое хранения для базы данных IBM Spectrum Protect, если измерять ее в операциях ввода-вывода в секунду (input/output operations per second, IOPS)?	Используйте для базы данных высокопроизводительный диск. Используйте технологию твердотельных дисков для обработки дедупликации данных. Убедитесь, что база данных обеспечивает минимальное значение в 3000 IOPS. Для каждого терабайта данных, копируемого в день (до дедупликации данных) прибавьте к этому минимуму 1000 IOPS. Например, для сервера IBM Spectrum Protect, который пропускает 3 ТБ данных в день, потребуется 6000 IOPS для дисков базы данных: `минимум 3000 IOPS + 3000 (3 ТБ x 1000 IOPS) = 6000 IOPS`	Рекомендации относительно выбора диска смотрите в разделе "Планирование для дисков базы данных сервера." Дополнительные сведения об IOPS смотрите в документах IBM Spectrum Protect Макеты.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Достаточно ли памяти для размера вашей базы данных?	Для серверов IBM Spectrum Protect с размером базы данных, равным 100 ГБ, которые производят дедупликацию данных, используйте, как минимум, 40 ГБ системной памяти. Если сохраняемый объем данных резервных копий возрастает, может понадобиться увеличить требования к системной памяти. Регулярно отслеживайте использование памяти, чтобы определить, не требуется ли дополнительная память. Используйте больше памяти, чтобы улучшить кэширование страниц базы данных. Приведенные ниже рекомендация по размеру памяти основаны на ежедневном объеме новых данных, резервные копии которых вы создаете: • 128 ГБ системной памяти для ежедневных резервных копий данных, когда размер базы данных равен 1-2 ТБ • 192 ГБ системной памяти для ежедневных резервных копий данных, когда размер базы данных равен 2-4 ТБ	Требования к памяти

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Правильно ли вы подобрали размер емкости хранения для активного и архивного журналов базы данных?	Сконфигурируйте для сервера минимальный размер активного журнала 128 ГБ, задав для опции сервера **ACTIVELOGSIZE** значение 131072. Рекомендуемый начальный размер архивного журнала - 1 ТБ. Размер архивного журнала ограничен размером файловой системы, в которой он находится, а не опцией сервера. Убедитесь, что для файловой системы есть хотя бы 10% дополнительного пространства на диске, превышающего размер архивного журнала. Используйте для архивных журналов баз данных каталог с начальной свободной емкостью, как минимум, 1 ТБ. Задайте каталог при помощи опции сервера **ARCHLOGDIRECTORY**. Определите пространство для архивного журнала восстановления после отказа при помощи опции сервера **ARCHFAILOVERLOGDIRECTORY**.	Дополнительную информацию о том, как подобрать размер системы, смотрите в документах IBM Spectrum Protect Макеты.
Включено ли сжатие для архивного журнала и резервных копий базы данных?	Включите опцию сервера ARCHLOGCOMPRESS, чтобы сэкономить пространство хранения. Эта опция сжатия отличается от строенного сжатия. Встроенное сжатие по умолчанию включено в IBM Spectrum Protect V7.1.5 и новее. **Ограничение:** Не используйте эту опцию, если объем резервных копий данных превышает 6 ТБ в день.	Дополнительную информацию о сжатии для вашей системы смотрите в документах IBM Spectrum Protect Макеты.
Расположены ли база данных и журналы IBM Spectrum Protect в разных томах диска (LUN)? Сконфигурирован ли диск, который используется для базы данных, в соответствии с рекомендациями для транзакционной базы данных?	База данных не должна использовать дисковые тома совместно с журналами или пулами хранения IBM Spectrum Protect, с другим приложением или с другой файловой системой.	Дополнительную информацию о базе данных сервера и конфигурации журнала восстановления смотрите в документе Конфигурирование и настройка базы данных сервера и журнала восстановления.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Используете ли вы, как минимум, восемь (2,2 ГГц или эквивалент) ядер процессора для каждого сервера IBM Spectrum Protect, который вы хотите использовать в сочетании с дедупликацией данных?	Если планируется использование дедупликации данных на стороне клиента, проверьте, есть ли у систем клиентов адекватные ресурсы, доступные во время операции резервного копирования, чтобы выполнять обработку дедупликации данных. Используйте процессор, эквивалентный по крайней мере одному процессорному ядру 2,2 ГГц, на каждый процесс резервного копирования с дедупликацией данных на стороне клиента.	• Дедупликация данных - Часто задаваемые вопросы • IBM Spectrum Protect Макеты
Выделен ли вами достаточный объем пространства хранения для базы данных?	В первом приближении нужно запланировать выделение 100 ГБ для хранения базы данных на каждые 25 ТБ данных, которые будут защищены в дедуплицированных пулах хранения. *Защищенные данные* - это объем данных перед дедупликацией данных, включая все версии сохраненных объектов. Для операций резервного копирования базы данных с большим числом мелких файлов, где средний размер файла меньше 512 КБ, требуется больше пространства базы данных. Для меньших размеров объектов запланируйте 100 ГБ пространства базы данных для каждых сохраненных 10 ТБ. Лучше всего задать новый пул хранения исключительно для дедупликации данных. Дедупликация данных производится на уровне пула хранения. Дедупликации подвергаются все данные, содержащиеся в пуле хранения, за исключением зашифрованных данных.	Оптимальная среда IBM Spectrum Protect настраивается с использованием IBM Spectrum Protect Макеты.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Оценили ли вы емкость пула хранения для конфигурирования достаточного пространства, соответствующего размеру вашей среды?	Для оценки требований к емкости для дедуплицированного пула хранения можно использовать следующий метод: 1. Оцените базовый размер данных источника. 2. Оцените ежедневный размер резервных копий, используя предполагаемый темп изменений и роста. 3. Определите требования к сроку хранения. 4. Вычислите общий размер данных данных источника с учетом базового размера, ежедневного размера резервных копий и требований к сроку хранения. 5. Примените коэффициент дедупликации. 6. Примените коэффициент сжатия. 7. Округлите оценку, чтобы учесть переходное использование пула хранения.	Пример использования этого метода смотрите на веб-странице Дедупликация данных - Часто задаваемые вопросы.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Распределили ли вы операции дискового ввода-вывода по нескольким дисковым устройствам и контроллерам?	Используйте массивы, которые состоят из как можно большего количества дисков (иногда это называется 'широкое чередование'. Убедитесь, что вы используете один каталог базы данных для отдельного массива в подсистеме. Задайте переменную реестра *DB2_PARALLEL_IO*, так чтобы включить параллельный ввод-вывод для каждого табличного пространства, используемого, если контейнеры в табличном пространстве охватывают несколько физических дисков. Если полоса пропускания для ввода-вывода доступна, а размер файлов велик (например, 1 МБ), процесс нахождения дубликатов может использовать ресурсы всего процессора. Когда файлы меньше, более критичны другие узкие места. Задайте восемь или больше файловых систем для класса устройств дедуплицированного пула хранения, чтобы операции ввода-вывода распределялись по максимально возможному числу LUN и физических устройств.	Рекомендации по настройке пулов хранения смотрите в разделе "Планирование для пулов хранения на устройствах классов устройств DISK или FILE." Информацию о настройке переменной *DB2_PARALLEL_IO* смотрите в документе Рекомендуемые параметры для переменных реестра IBM Db2.
Запланировали ли вы ежедневные операции на основе вашей стратегии резервного копирования?	Наилучшая последовательность операций будет следующей: 1. Резервное копирование клиента 2. Защита пула хранения 3. Репликация узлов 4. Резервное копирование базы данных 5. Окончание действия устаревших файлов	• Планирование дедупликации данных и процессов репликации узла • Ежедневные операции для пулов хранения каталогов-контейнеров

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Запланировали ли вы операции аудита, чтобы выявить поврежденные файлы в пулах хранения?	Чтобы запланировать операции аудита, используйте команду **DEFINE STGRULE** с параметром **ACTIONTYPE=AUDIT**. Исходя из передовой практики, чтобы убедиться, что операции аудита выполняются постоянно, не задавайте параметр **DELAY**.	
Достаточно ли у вас пространства хранения для управления списком блокировки IBM Db2?	Если выполняется дедупликация данных, в состав которых входят большие объекты или большое число одновременно обрабатываемых файлов, процесс может привести к тому, что станет не хватать пространства хранения. При нехватке пространства хранения списка блокировок могут происходить ошибки резервного копирования, отказы процессов управления данными или перерывы в работе сервера. Если дедупликация данных обрабатывает файлы размером более 500 ГБ, это вероятнее всего приведет к истощению пространства хранения. Но если большое число выполняемых операций резервного копирования использует дедупликацию данных на стороне клиента, эта проблема может также произойти и с файлами меньшего размера.	Информацию о настройке параметра Db2 **LOCKLIST** смотрите в документе Настройка дедупликации данных на стороне сервера.
Доступна ли достаточная полоса пропускания для передачи данных на сервер IBM Spectrum Protect?	Чтобы переносить данные на сервер IBM Spectrum Protect, используйте дедупликацию данных на стороне клиента или на стороне сервера и сжатие, чтобы уменьшить необходимую ширину полосы пропускания. Используйте сервер V7.1.5 или новее, чтобы применить встроенное сжатие, и используйте клиент V7.1.6 или новее, чтобы включить усовершенствованную обработку сжатия.	Дополнительные сведения смотрите в описании опции клиента **enablededup**.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Определили ли вы, сколько каталогов пула хранения следует назначить для каждого пула хранения?	Назначьте каталоги для пула хранения, используя команду **DEFINE STGPOOLDIRECTORY**. Создайте несколько каталогов пула хранения и убедитесь, что для каждого каталога создается резервная копия на отдельном дисковом томе (LUN).	
Выделен ли вами достаточный объем дискового пространства в пуле хранения облачных контейнеров?	Чтобы предотвратить ошибки резервного копирования, убедитесь, что в локальном каталоге достаточно места. Оптимальный размер дискового пространства указан ниже в списке: • Для SCSI с последовательным подключением (SAS) и вращающегося диска вычислите объем новых данных, ожидаемых поле ежедневного сокращения объема данных (сжатие и дедупликация данных). Выделите до 100 процентов этого количества в терабайтах для дискового пространства. • Для систем хранения на основе флеш-памяти, у которых есть быстрые сетевые соединения с высокопроизводительными облачными системами, требуется 3 ТБ. • Для систем хранения с твердотельными накопителями (SSD), у которых есть быстрые сетевые соединения с высокопроизводительными облачными системами, требуется 5 ТБ.	

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Выбрали ли вы подходящий тип локальной системы хранения?	Убедитесь, что передача данных из локальной системы хранения в облако завершена до начала следующего цикла резервного копирования. **Совет:** Данные удаляются из локальной системы хранения вскоре после их перемещения в облако. Учтите следующие рекомендации: • Используйте флеш-память или твердотельные накопители (SSD) для больших облачных система высокой производительности. Убедитесь, что у вас есть ссылка на глобальную сеть (wide area network, WAN) с выделенными 10 ГБ памяти и высокоскоростным соединением с системой хранения объектов. Например, используйте флеш-память или SSD, если у вас выделенная ссылка 10 ГБ WAN плюс высокоскоростное соединение либо с положением IBM Cloud Object Storage, либо с центром данных Amazon Simple Storage Service (Amazon S3). • Для указанных ниже сценариев используйте диски SAS большей емкости 15000 rpm: – Системы среднего размера – Медленные соединения с облаком, например 1 ГБ – При использовании IBM Cloud Object Storage в качестве провайдера службы в нескольких регионах • Для SAS или вращающегося диска вычислите объем новых данных, ожидаемых после ежедневного сокращения объема данных (сжатие и дедупликация данных). Выделите до 100 процентов этого количества в терабайтах для дискового пространства.	

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Задали ли вы общее максимальное число параллельных процессов для правила хранения и для каждого из его субправил для пулов хранения облачного контейнера?	Чтобы задать максимальное число параллельных процессов, введите команду **DEFINE STGRULE**, указав значение параметра **MAXPROCESS**. Значение по умолчанию - 8. Например, если задано значение по умолчанию 8, а правило хранения состоит из четырех субправил, то правило хранения может запустить восемь параллельных процессов, и каждое из его субправил может запустить восемь параллельных процессов. Чтобы обеспечить оптимальную пропускную способность, используйте следующее максимальное число параллельных процессов для малых, средних и больших систем Blueprint: • Малая система: 10 процессов • Средняя система: 25 процессов • Большая система: 35-50 процессов	
Вы задали для пулов хранения облачных контейнеров несколько конечных точек Accesser, если вы используете локальную систему IBM Cloud Object Storage с IBM Spectrum Protect?	Чтобы оптимизировать производительность, задайте для малых, средних и больших систем монопольное (исключительное) право доступа для указанного числа Клиенты доступа в зависимости от ваших требований к поглощению данных: • Небольшая система: 1 Accesser • Средняя система: 2 Клиенты доступа • Крупная система: 3-4 Клиенты доступа	Дополнительную информацию смотрите на веб-сайте IBM Spectrum Protect Cloud Blueprints.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Вы задали для пулов хранения облачных контейнеров несколько конечных точек Accesser, если вы используете локальную систему IBM Cloud Object Storage с IBM Spectrum Protect?	В общем случае для соединения с частными конечными точками IBM Cloud Object Storage для малых, средних и крупных систем Blueprint требуется следующая поддержка Ethernet: • Малая система: 1 Гбит • Средняя система: 5 Гбит • Крупная система: 10 Гбит **Совет:** В зависимости от поглощения данных клиентом и одновременной передачи данных в систему хранения объектов может потребоваться сеть с пропускной способностью, большей, чем у одной 10-Гбайтной сети Ethernet. При конфигурировании соединения Ethernet работайте вместе с сетевым администратором и рассмотрите следующие факторы: • Возможности поддержки Ethernet сервером • Характер сети между сервером и конечной точкой IBM Cloud Object Storage • Конечная точка поглощения в системе хранения объектов через пул хранения облачного контейнера	

Планирование для пулов хранения на устройствах классов устройств DISK или FILE

Используйте контрольный список, чтобы проверить, как настроены дисковые пулы хранения. Этот контрольный список содержит советы для пулов хранения, использующих классы устройств DISK или FILE.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Могут ли LUN пула хранения поддерживать пропускную способность для последовательного чтения и записи, объемом 256 КБ, чтобы адекватно обрабатывать рабочую нагрузку в пределах ограничений времени?	При планировании пиковых нагрузок учитывайте все данные, которые сервер должен читать из дисковых пулов хранения или записывать в дисковые пулы хранения одновременно. Например, рассмотрим пиковый поток данных от одновременно выполняющихся операций резервного копирования клиента и операций по перемещению данных сервером, например, перенастройку. В подавляющем большинстве случаев сервер IBM Spectrum Protect производит чтение из пулов хранения и записывает данные в пулы хранения блоками по 156 КБ. Если дисковая система обеспечивает такую возможность, сконфигурируйте дисковую систему для оптимальной производительности при выполнении последовательных операций чтения/записи, а не случайных операций чтения/записи.	Дополнительную информацию смотрите в документе Анализ базовой производительности дисковых систем.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Выделен ли вами достаточный объем пространства хранения для базы данных?	Ниже приведены рекомендации по размеру базы данных на основе небольших, средних и больших систем, которые можно использовать для роста базы данных: • Небольшая система: не менее 1 ТБ • Средняя система: не менее 2 ТБ • Крупная система: не менее 4 ТБ **Совет:** Может потребоваться больше памяти в зависимости от объема данных, которые нужно защищать, числа сохраняемых файлов и от того, используется ли дедупликация данных. При дедупликации данных нагрузка на базу данных становится больше, так как в этом случае часто используются адресованные базе данных запросы, чтобы определить, какие дедуплицированные экстенты есть на сервере. В первом приближении нужно запланировать выделение 100 ГБ для хранения базы данных на каждые 50 ТБ данных, которые будут защищены в дедуплицированных пулах хранения. Защищенные данные - это объем данных перед дедупликацией данных, включая все версии сохраненных объектов. Если у вас есть несколько сот ТБ защищенных данных или если вы ежедневно создаете резервные копии многих ТБ данных, начальный размер базы данных должен составлять хотя бы 1 ТБ. Чтобы определить размер базы данных для вашей системы, используйте IBM Spectrum Protect.	Оптимальная среда IBM Spectrum Protect настраивается с использованием IBM Spectrum Protect Макеты. Информацию о минимальном объеме памяти, который необходимо выделить на сервере для выполнения операций, на основе размера базы данных смотрите в разделе Требования к памяти.
Сконфигурирован ли диск для использования кэша чтения и записи?	Используйте больший объем кэша, чтобы повысить производительность.	

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Вам требуется сделать резервную копию базы данных IBM Spectrum Protect в облачную систему хранения объектов?	Можно сделать резервную копию базы данных в облачную систему хранения объектов для целей восстановления при авариях и восстановить базу данных из нее. Вы можете настроить конечные точки системы хранения объектов, IBM Cloud Object Storage Клиенты доступа, пропускную способность сети и потоки данных, чтобы обеспечить эффективность операций резервного копирования баз данных.	Настройка резервных копий базы данных для использования хранения облачных объектов.
Определили ли вы правильный размер, который следует использовать для томов пула хранения, когда пулы хранения используют класс устройств FILE?	Ознакомьтесь с информацией в разделе Оптимальное число и размер томов для пулов хранения, использующих диск. Если у вас нет информации, которая бы позволила оценить размер томов класса устройств FILE, начните с томов, имеющих 50 ГБ.	Как правило, проблемы чаще возникают, если тома слишком малы. Если тома больше, чем требуется, сообщается о малом числе проблем. Когда вы определите размер тома, который следует использовать, в качестве предосторожности выберите размер, который может оказаться больше необходимого.
Используете ли вы заранее выделенные тома для пулов хранения, использующих классы устройств FILE?	Чистые тома могут вызвать фрагментацию файлов. Чтобы убедиться, что пулу хранения будет хватать томов, задайте для параметра **MAXSCRATCH** значение больше нуля.	Используйте серверную команду **DEFINE VOLUME**, чтобы заранее выделить тома в пуле хранения. Используйте серверную команду **DEFINE STGPOOL** или **UPDATE STGPOOL**, чтобы задать параметр **MAXSCRATCH**.
Сравнивали ли вы максимальное число сеансов клиентов с числом заданных томов для пулов хранения, использующих классы устройств FILE?	Всегда оставляйте в пулах хранения достаточное число пригодных для использования томов, чтобы разрешить одновременное выполнение ожидаемого пикового числа сеансов клиентов. Тома могут быть чистыми, пустыми или частично заполненными томами.	В случае пулов хранения, которые используют класс устройств FILE, на том одновременно может производить запись только один сеанс или процесс.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Задали ли вы для параметра **MOUNTLIMIT** класса устройств достаточно высокое значение, чтобы учесть число томов, которые могут быть смонтированы параллельно, когда пулы хранения используют класс устройств FILE?	Для пулов хранения, использующих дедупликацию данных, параметр **MOUNTLIMIT**, как правило, находится в диапазоне 500-1000. Задайте для **MOUNTLIMIT** значение, равное максимальному числу необходимых точек монтирования, необходимых для всех активных сеансов. Рассмотрим параметры, которые влияют на максимальное число необходимых точек монтирования: • Опция сервера **MAXSESSIONS**, представляющая собой максимальное число сеансов IBM Spectrum Protect, которые могут выполняться одновременно. • Параметр **MAXNUMMP**, указывающий, какое максимальное число точек монтирования может использовать каждый клиентский узел. Например, если максимальное число сеансов резервного копирования клиентских узлов, как правило, составляет 100, а для каждого из узлов задан параметр MAXNUMMP=2, умножьте 100 узлов на 2 точки монтирования для каждого узла, чтобы получить значение 200 для параметра **MOUNTLIMIT**.	Используя серверную команду **REGISTER NODE** или **UPDATE NODE**, задайте параметр **MAXNUMMP** для клиентских узлов.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Определили ли вы, сколько томов пула хранения поместить в каждую файловую систему для пулов хранения, использующих классы устройств DISK?	То, как вы конфигурируете пространство хранения для пула хранения, использующего класс устройств DISK, зависит от того, используете ли вы RAID для дисковой системы. Если вы не используете RAID, сконфигурируйте по одной файловой системе на физический диск и задайте по одному тому пула хранения для каждой файловой системы. Если вы используете RAID 5 с *n*+1 томами, сконфигурируйте пространство хранения одним из следующих способов: • Сконфигурируйте *n* файловых систем на LUN и задайте по одному тому пула хранения для файловой системы. • Сконфигурируйте одну файловую систему и *n* томов пула хранения для LUN.	Пример схемы, соответствующей этой рекомендации, смотрите в документе Пример схемы пулов хранения сервера.
Создали ли вы пулы хранения для распределения операций ввода-вывода по нескольким файловым системам?	Убедитесь, что каждая файловая система находится на отдельном LUN в дисковой системе. Как правило, 10-30 файловых систем - это оптимальная цель, но вы должны убедиться, что размер файловых систем будет не менее, чем 250 ГБ (примерно).	Дополнительные сведения смотрите в следующих разделах: • Настройка дискового хранения для сервера • Настройка и конфигурирование пулов хранения и томов
Запланировали ли вы операции аудита, чтобы выявить поврежденные файлы в пулах хранения?	Чтобы запланировать операции аудита, используйте команду **DEFINE STGRULE** с параметром **ACTIONTYPE=AUDIT**. Чтобы помочь оптимизировать операции аудита и обеспечить их непрерывную работу, не задавайте параметр **DELAY**.	

Планирование правильного типа технологии хранения

У устройств хранения разные характеристики емкости и производительности. Эти характеристики влияют на то, какие устройства лучше всего использовать в сочетании с IBM Spectrum Protect.

Процедура

- Ознакомьтесь со следующей таблицей, которая поможет вам выбрать правильный тип технологии хранения для ресурсов хранения, необходимых серверу.

Таблица 5. Типы технологии хранения в требованиях по хранению IBM Spectrum Protect

Тип технологии хранения	**База данных**	**Активный журнал**	**Архивный журнал и резервный архивный журнал**	**Пулы хранения**
Твердотельный диск (Solid-state disk, SSD)	Размещайте базу данных на SSD при следующих обстоятельствах: – Вы используете дедупликацию данных IBM Spectrum Protect. – Вы ежедневно производите резервное копирование более чем 8 ТБ новых данных.	Если вы поместите базу данных IBM Spectrum Protect на SSD, лучше всего поместить активный журнал на SSD. Если пространство недоступно, используйте вместо этого высокопроизводит. диск.	Оставьте накопители SSD для использования в сочетании с базой данных и активным журналом. Архивный журнал и архивные журналы передачи управления при отказе можно поместить на носители с более медленными типами технологии хранения.	Оставьте накопители SSD для использования в сочетании с базой данных и активным журналом. Пулы хранения можно поместить на носители с более медленными типами технологии хранения.
Высокопроизв. диск со следующими хар-ками: **– Диск 15 K rpm** **– Оптовол. (Fibre Channel) интерфейс или последов. подкл. интерфейс SCSI (SAS).**	Используйте высокопроизв. диски при следующих обстоятельствах: – Сервер не производит дедупликацию данных. – Сервер не производит репликацию узлов. Изолируйте базу данных сервера от ее журналов и пулов хранения и от данных для других приложений.	Используйте высокопроизв. диски при следующих обстоятельствах: – Сервер не производит дедупликацию данных. – Сервер не производит репликацию узлов. Чтобы обеспечить достаточный уровень производительности и доступности, изолируйте активный журнал от базы данных сервера, от архивных журналов и пулов хранения.	Высокопроизв. диски можно использовать для архивного журнала и архивных журналов передачи управления при отказе. Чтобы обеспечить доступность, изолируйте эти журналы от базы данных и активного журнала.	Используйте высокопроизв. диски для пулов хранения при следующих обстоятельствах: – Данные часто читаются. – Данные часто записываются. Чтобы обеспечить достаточный уровень производительности и доступности, изолируйте данные пула хранения от базы данных сервера и от данных для других приложений.

Таблица 5. Типы технологии хранения в требованиях по хранению IBM Spectrum Protect (продолжение)

Тип технологии хранения	База данных	Активный журнал	Архивный журнал и резервный архивный журнал	Пулы хранения
Диск средней произв. или высокопроизв. диск со следующими хар-ками: **– Диск 10 K rpm** **– Оптовол. (Fibre Channel) интерфейс или интерфейс SAS**	Если дисковая система представляет собой смесь дисковых технологий, используйте более быстрые диски для базы данных и активного журнала. Изолируйте базу данных сервера от ее журналов и пулов хранения и от данных для других приложений.	Если дисковая система представляет собой смесь дисковых технологий, используйте более быстрые диски для базы данных и активного журнала. Чтобы обеспечить достаточный уровень производительности и доступности, изолируйте активный журнал от базы данных сервера, от архивных журналов и пулов хранения.	Диск средней производительности или высокопроизв. диск можно использовать для архивного журнала и архивных журналов передачи управления при отказе. Чтобы обеспечить доступность, изолируйте эти журналы от базы данных и активного журнала.	Используйте диск средней производительности или высокопроизв. диск для пулов хранения при следующих обстоятельствах: – Данные часто читаются. – Данные часто записываются. Чтобы обеспечить достаточный уровень производительности и доступности, изолируйте данные пула хранения от базы данных сервера и от данных для других приложений.
SATA, пространство хранения, подключенное к сети	Не используйте этот тип хранения для базы данных. Не помещайте базу данных в системы хранения XIV.	Не используйте этот тип хранения для активного журнала.	Использование этой более медленной технологии хранения является приемлемым, так как эти журналы записываются один раз и редко читаются.	Используйте эту более медленную технологию хранения при следующих обстоятельствах: – Данные редко записываются, например, записываются один раз. – Данные редко читаются. .
Лента и виртуальная лента				Используйте для долгосрочного хранения, если данные используются нечасто.

Применение наилучших практических методов к установке сервера

Как правило, конфигурация и выбор оборудования оказывают наиболее значительное влияние на производительность решения IBM Spectrum Protect. Другими факторами, влияющими на

производительность, являются выбор и конфигурация операционной системы, а также конфигурация IBM Spectrum Protect.

Процедура

- Описанные ниже наилучшие методы являются наиболее важными для достижения оптимальной производительности и предотвращения ошибок.
- Смотрите таблицу, чтобы определить наилучшие методы, применимые к вашей среде.

Практическая рекомендация	**Дополнительная информация**
Используйте для базы данных сервера быстрые диски. Твердотельные диски (solid-state disks, SSD) уровня предприятия с оптоволоконным интерфейсом или интерфейсом SAS предлагают наивысшую производительность.	Используйте для базы данных быстрые диски с низкой латентностью. Использование SSD является существенным, если вы используете дедупликацию данных и репликацию узлов. Старайтесь не использовать диски Serial Advanced Technology Attachment (SATA) и Parallel Advanced Technology Attachment (PATA). Подробную информацию и дополнительные советы смотрите в следующих разделах: – "Планирование дисков базы данных сервера" – "Планирование правильного типа технологии хранения"
Убедитесь, что в системе сервера достаточно памяти.	Прочтите требования к операционной системе в техническом замечании 1243309. При более высоких рабочих нагрузках требуется больше ресурсов, чем указано в минимальных требованиях. Такие дополнительные функции, как дедупликация данных и репликация узлов, могут потребовать объем памяти, превышающий минимальный объем, указанный в документе с требованиями к системе. Если вы планируете запускать несколько экземпляров сервера, каждому экземпляру потребуется объем памяти, указанный для одного сервера. Умножьте объем памяти для одного сервера на число экземпляров, которые вы собираетесь запускать в системе.
Отделите базу данных сервера, активный журнал, архивный журнал и дисковые пулы хранения друг от друга.	Держите все ресурсы хранения IBM Spectrum Protect на отдельных дисках. Держите диски пулов хранения храниться отдельно от дисков базы данных сервера и журналов. Операции пулов хранения могут перекрываться операциями базы данных, если они находятся на одних и тех же дисках. В идеале база данных сервера и журналы также должны быть отделены друг от друга. Подробную информацию и дополнительные советы смотрите в следующих разделах: – "Планирование дисков базы данных сервера" – "Планирование для дисков журнала восстановления сервера" – "Планирование для пулов хранения на устройствах классов устройств DISK или FILE"

Практическая рекомендация	Дополнительная информация
Используйте для базы данных сервера хотя бы четыре каталога. Для больших серверов или серверов, использующих дополнительные функции, используйте восемь каталогов.	Поместите каждый каталог на LUN, изолированный от других LUN и от других приложений. Сервер считается большим, если его база данных превышает 2 ТБ или если ожидается, что она вырастет больше этого размера. Используйте для таких серверов восемь каталогов. Смотрите раздел "Планирование для дисков базы данных сервера."
Если вы используете дедупликацию данных и/или репликацию узлов, следуйте рекомендациям по конфигурированию базы данных и других элементов.	Сконфигурируйте базу данных сервера в соответствии с рекомендациями, так как база данных чрезвычайно важна для того, чтобы сервер смог хорошо работать, если используются такие функции. Подробную информацию и дополнительные советы смотрите в следующих разделах: – Контрольный список для дедупликации данных – Контрольный список по репликации узлов
В случае пулов хранения, которые используют класс устройств типа FILE, выполните рекомендации по размеру томов пула хранения. Как правило, тома 50 ГБ подходят лучше всего.	Прочтите информацию в разделе Оптимальное число и размер томов для пулов хранения, использующих диск, чтобы это помогло вам определить размер тома. Сконфигурируйте устройства пула хранения и файловые системы на основе требований к пропускной способности, а не только на основе требований к емкости. Изолируйте устройства хранения, используемые продуктом IBM Spectrum Protect, от других приложений с высоким объемом ввода-вывода и убедитесь, что для этой системы хранения обеспечивается достаточная пропускная способность. Дополнительные сведения смотрите в разделе Контрольный список для пулов хранения на устройствах DISK или FILE.
Запланируйте операции клиента IBM Spectrum Protect и действия по обслуживанию сервера, чтобы избежать перекрывания операций или свести такое перекрывание к минимуму.	Дополнительные сведения смотрите в следующих разделах: – Настройка расписания для ежедневных операций – Контрольный список для конфигурации сервера
Постоянно осуществляйте мониторинг операций.	Проводя мониторинг, вы сможете раньше находить ошибки и вам будет проще выявлять их причины. Срок хранения записей отчетов мониторинга может доходить до года - это поможет вам выявлять тенденции и планировать рост. Смотрите раздел Мониторинг среды и ее обслуживание с целью обеспечения производительности.

Минимальные требования к системе

Чтобы установить сервер IBM Spectrum Protect в системе Linux, требуется минимальный уровень аппаратного и программного обеспечения, включая способ связи и самую последнюю версию драйверов устройств.

Оптимальная среда IBM Spectrum Protect настраивается с дедупликацией данных с использованием IBM Spectrum Spectrum Protect Blueprints.

Пакет драйверов устройств IBM Spectrum Protectne содержит драйвер устройств для этой операционной системы, так как используется типовой драйвер устройств SCSI. Сконфигурируйте

драйвер устройств до использования сервера IBM Spectrum Protect с ленточными устройствами. Пакет драйверов IBM Spectrum Protect содержит инструменты драйверов и демоны ACSLS. Найти драйверы устройств IBM можно на сайте Fix Central.

Требования, информация о поддерживаемых устройствах, пакеты установки клиента и исправления можно получить по адресу: Портал подержки IBM для IBM Spectrum Protect. После установки IBM Spectrum Protect и до настройки этого продукта посетите этот веб-сайт и скачайте и примените все применимые исправления.

Минимальные требования к серверу Linux x86_64

Прежде чем устанавливать сервер IBM Spectrum Protect в операционной системе Linux x86_64, ознакомьтесь с требованиями к аппаратному и программному обеспечению.

Требования к аппаратному и программному обеспечению для установки сервера IBM Spectrum Protect

Самую последнюю информацию о требованиях к системе IBM Spectrum Protect смотрите в техническом замечании 84861.

В таблице 1 приводятся минимальные требования к аппаратному обеспечению, необходимому для сервера в системе Linux x86_64.

Таблица 6. Требования к аппаратным средствам

Тип аппаратуры	**Требования к аппаратным средствам**
Общее	Процессор AMD64 или Intel EM64T

Таблица 6. Требования к аппаратным средствам (продолжение)

Тип аппаратуры	Требования к аппаратным средствам
Дисковое пространство	Следующие минимальные объемы дискового пространства: • 4.3 ГБ для каталога установки • 2.5 ГБ для каталога `/var` • 4 ГБ для каталога `/tmp` • 128 МБ для домашнего каталога для пользователя root • 2 ГБ для области совместно используемых ресурсов Если возникнет проблема и потребуется какая-либо диагностика, оптимальным является, чтобы в системе было доступно временное или другое пространство для журнала захвата данных первой ошибки (first failure data capture, FFDC) или для другого временного использования, например, для сбора журналов трассировки. Для базы данных и файлов журналов дополнительно требуется значительный объем дискового пространства. Размер базы данных зависит от количества клиентских файлов, которые необходимо хранить, и метода, с помощью которого сервер управляет ими. Объем пространства активного журнала по умолчанию равен 16 ГБ; это необходимый минимум для большинства рабочих нагрузок и конфигураций. При создании активного журнала нужно, по крайней мере, 64 ГБ для выполнения репликации. Если используются и репликация, и дедупликация данных, создайте активный журнал, размер которого будет равен 128 ГБ. Выделите для архивного журнала, как минимум, в три раза больший объем пространства, чем для активного журнала по умолчанию (48 ГБ). Если вы используете дедупликацию данных или ожидаете высокий уровень рабочей нагрузки на клиент, убедитесь, что у вас достаточно ресурсов. Чтобы обеспечить оптимальную производительность и эффективность ввода-вывода, задайте, как минимум, два контейнера с одинаковым размером или с одинаковыми номерами Logical Unit Number (LUN), которые будут использоваться базой данных. Кроме того, для каждого активного журнала и архивного журнала нужен свой собственный контейнер или LUN. Обязательно ознакомьтесь с более подробной информацией о дисковом пространстве в разделе “Планирование емкости” на стр. 62.
Память	Следующие минимальные объемы памяти: • 16 ГБ для стандартных операций сервера без дедупликации данных и репликации узлов • 24 ГБ для дедупликации данных или репликации узлов • 32 ГБ для репликации узлов с дедупликацией данных Более конкретные требования к памяти для более крупных баз данных и большей возможности поглощения смотрите в документе Таблица настройки памяти сервера IBM Spectrum Protect. Особые требования к памяти, когда используется дедупликация данных, смотрите в документе IBM Spectrum Protect Blueprint для вашей операционной системы.

Требования к программному обеспечению

В таблице 2 приводятся минимальные требования к программному обеспечению, необходимому для сервера в системе Linux x86_64.

Таблица 7. Требования к программному обеспечению

Тип программного обеспечения	**Минимальные требования к программному обеспечению**
Операционная система	Для работы сервера IBM Spectrum Protect в системе Linux x86_64 требуется одна из следующих операционных систем: • Red Hat Enterprise Linux 8.1 или новее • Red Hat Enterprise Linux 7.6 или новее • SUSE Linux Enterprise Server 15, SP1 или новее • SUSE Linux Enterprise Server 12, SP4 или новее • Ubuntu Server LTS версии 16.04.2 или 18.04. В случае ленточного хранения минимальной версией Ubuntu Server LTS является версия 18.04.
Библиотеки	Библиотеки GNU C версии 2.3.3-98.38 или новее, установленные в системе IBM Spectrum Protect. Для серверов Red Hat Enterprise Linux: • libaio • libstdc++.so.6 (требуются 32- и 64-битные пакеты) • numactl.x86_64 Для Red Hat Enterprise Linux (RHEL 8) добавьте также следующую библиотеку: • libnsl.so.1 • libnuma.so.1 Для серверов SUSE Linux Enterprise: • libaio • libstdc++.so.6 версии 4.3 или новее (требуются 32- и 64-битные пакеты) • libnuma.so.1 Для серверов Ubuntu LTS Server: • libaio1 • libnuma.so.1 Чтобы определить, установлен ли SELinux и включен ли режим принудительного применения, выполните одно из следующих действий: • Проверьте файл `/etc/sysconfig/selinux`. • Введите команду операционной системы **`sestatus`**. • Проверьте наличие в файле `/var/log/messages` сообщений SELinux. **Ограничение:** Для установок и обновления IBM Spectrum Protect нужно отключить SELinux. Чтобы отключить SELinux, выполните одну из следующих задач: • Задайте режим permissive, введя команду `setenforce 0` от имени суперпользователя. • Измените файл `/etc/sysconfig/selinux` и перезапустите компьютер.
Протокол связи	• TCP/IP V4 или V7, входящий в стандартный комплект поставки Linux • Протокол Shared Memory (при использовании клиента IBM Spectrum Protect (клиент Linux x86_64)

Таблица 7. Требования к программному обеспечению (продолжение)

Тип программного обеспечения	Минимальные требования к программному обеспечению
Обработка	Должен быть включен асинхронный ввод-вывод. В системе Linux с ядром версии 2.6 и новее для включения асинхронного ввода-вывода установите библиотеку libaio.
Драйверы устройств	Промежуточный драйвер устройств IBM Spectrum Protect используется для устройств, изготовленных не IBM. Он использует промежуточный интерфейс SCSI для связи с ленточными устройствами и ленточными библиотеками. Для ленточных накопителей и ленточных библиотек рекомендуется использовать драйвер устройств Linux SCSI Generic (sg). Пакет драйверов устройств IBM Spectrum Protect содержит инструменты драйверов устройств и демоны ACSLS. Для ленточных библиотек или накопителей IBM 3590, 3592 или Ultrium требуются драйверы устройств IBM. Установите самые свежие драйверы устройств. Вы можете найти пакеты драйверов IBM на странице Fix Central. Сконфигурируйте драйверы устройств до использования сервера IBM Spectrum Protect с ленточными устройствами.
Другое программное обеспечение	• Оболочка Korn (ksh) • Для аутентификации пользователей IBM Spectrum Protect посредством сервера Lightweight Directory Access Protocol нужно использовать один из следующих серверов каталогов: – Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2, Windows Server 2016) – IBM Security Directory Server V6.3 – IBM Security Directory Server V6.4

Минимальные требования к серверу Linux on System z

Прежде чем устанавливать сервер IBM Spectrum Protect в операционной системе Linux on System z, ознакомьтесь с требованиями к аппаратному и программному обеспечению.

Требования к аппаратному и программному обеспечению для установки сервера IBM Spectrum Protect

Самую последнюю информацию о требованиях к системе IBM Spectrum Protect смотрите в техническом замечании 1243309.

В таблице 1 приводятся минимальные требования к аппаратному обеспечению вашего компьютера IBM Spectrum Protect под управлением Linux on System z. Более подробную информацию о планировании объема дискового пространства смотрите в разделе “Планирование емкости” на стр. 62.

Таблица 8. Требования к аппаратным средствам

Тип аппаратуры	Требования к аппаратным средствам
Общее	An IBM zSeries, IBM System z9, IBM System z10 или IBM zEnterprise System (z114 и z196) с собственным 64-битным логическим разделом (logical partition, LPAR) или гостевой системой z/VM.

Таблица 8. Требования к аппаратным средствам (продолжение)

Тип аппаратуры	Требования к аппаратным средствам
Дисковое пространство	Следующие минимальные объемы дискового пространства: • 4.3 ГБ для каталога установки • 2.5 ГБ для каталога `/var` • 4 ГБ для каталога `/tmp` • 128 МБ для домашнего каталога для пользователя root • 2 ГБ для области совместно используемых ресурсов Если возникнет проблема и потребуется какая-либо диагностика, оптимальным является, чтобы в системе было доступно временное или другое пространство для журнала захвата данных первой ошибки (first failure data capture, FFDC) или для другого временного использования, например, для сбора журналов трассировки. Для базы данных и файлов журналов дополнительно требуется значительный объем дискового пространства. Размер базы данных зависит от количества клиентских файлов, которые необходимо хранить, и метода, с помощью которого сервер управляет ими. Объем пространства активного журнала по умолчанию равен 16 ГБ; это необходимый минимум для большинства рабочих нагрузок и конфигураций. При создании активного журнала нужно, по крайней мере, 64 ГБ для выполнения репликации. Если используются и репликация, и дедупликация данных, создайте активный журнал, размер которого будет равен 128 ГБ. Выделите для архивного журнала, как минимум, в три раза больший объем пространства, чем для активного журнала по умолчанию (48 ГБ). Если вы используете дедупликацию данных или ожидаете высокий уровень рабочей нагрузки на клиент, убедитесь, что у вас достаточно ресурсов. Чтобы обеспечить оптимальную производительность и эффективность ввода-вывода, задайте, как минимум, два контейнера с одинаковым размером или с одинаковыми номерами Logical Unit Number (LUN), которые будут использоваться базой данных. Кроме того, для каждого активного журнала и архивного журнала нужен свой собственный контейнер или LUN. Обязательно ознакомьтесь с более подробной информацией о дисковом пространстве в разделе “Планирование емкости” на стр. 62.
Память	Следующие минимальные объемы памяти: • 16 ГБ для стандартных операций сервера без дедупликации данных и репликации узлов • 24 ГБ для дедупликации данных или репликации узлов • 32 ГБ для репликации узлов с дедупликацией данных Более конкретные требования к памяти для более крупных баз данных и большей возможности поглощения смотрите в документе Таблица настройки памяти сервера IBM Spectrum Protect. Особые требования к памяти, когда используется дедупликация данных, смотрите в документе IBM Spectrum Protect Blueprint для вашей операционной системы.

Требования к программному обеспечению

В таблице 2 приводятся минимальные требования к программному обеспечению вашего компьютера под управлением IBM Spectrum Protect Linux on System z.

Таблица 9. Требования к программному обеспечению

Тип программного обеспечения	Минимальные требования к программному обеспечению
Операционная система	Для сервера IBM Spectrum Protect в Linux on System z (s390x 64-битная архитектура) требуется одна из следующих операционных систем: • Red Hat Enterprise Linux 7.6 или новее • SUSE Linux Enterprise Server 12, SP4 или новее **Ограничение:** Функция обнаружения сети хранения данных (storage area network, SAN) не поддерживается.
Библиотеки	Библиотеки GNU C версии 2.3.3-98.38 или новее, установленные в системе IBM Spectrum Protect. Для серверов Red Hat Enterprise Linux: • libaio • libstdc++.so.6 (требуются 32- и 64-битные пакеты) • libxlc-1.2.0.0.151119a.s390x или новее Для серверов SUSE Linux Enterprise: • libaio • libstdc++.so.6 версии 4.3 или новее (требуются 32- и 64-битные пакеты) • libxlc-1.2.0.0.151119a.s390x или новее Чтобы определить, установлен ли SELinux и включен ли режим принудительного применения, выполните одно из следующих действий: • Проверьте файл `/etc/sysconfig/selinux`. • Введите команду операционной системы **`sestatus`**. • Проверьте наличие в файле `/var/log/messages` сообщений SELinux. **Ограничение:** Для установок и обновления IBM Spectrum Protect нужно отключить SELinux. Чтобы отключить SELinux, выполните одну из следующих задач: • Задайте режим permissive, введя команду `setenforce 0` от имени суперпользователя. • Измените файл `/etc/sysconfig/selinux` и перезапустите компьютер.
Протокол связи	• TCP/IP V4 или V7, входящий в стандартный комплект поставки Linux • Протокол Shared Memory (при использовании клиента IBM Spectrum Protect (клиент Linux s390x)
Обработка	Должен быть включен асинхронный ввод-вывод. В системе Linux с ядром версии 2.6 и новее для включения асинхронного ввода-вывода установите библиотеку libaio.

Таблица 9. Требования к программному обеспечению (продолжение)

Тип программного обеспечения	Минимальные требования к программному обеспечению
Драйверы устройств	Промежуточный драйвер устройств IBM Spectrum Protect используется для устройств, изготовленных не IBM. Он использует промежуточный интерфейс SCSI для связи с ленточными устройствами и ленточными библиотеками. Для ленточных накопителей и ленточных библиотек рекомендуется использовать драйвер устройств Linux SCSI Generic (sg). Пакет драйверов устройств IBM Spectrum Protect содержит инструменты драйверов устройств и демоны ACSLS. Для ленточных библиотек или накопителей IBM 3590, 3592 или Ultrium требуются драйверы устройств IBM. Установите самые свежие драйверы устройств. Вы можете найти пакеты драйверов IBM на странице Fix Central. Сконфигурируйте драйверы устройств до использования сервера IBM Spectrum Protect с ленточными устройствами.
Другое программное обеспечение	• Оболочка Korn (ksh) • Для аутентификации пользователей IBM Spectrum Protect посредством сервера Lightweight Directory Access Protocol нужно использовать один из следующих серверов каталогов: – Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2, Windows Server 2016) – IBM Security Directory Server V6.3 – IBM Security Directory Server V6.4

Минимальные требования к серверу Linux on Power Systems (с прямым порядком байтов)

Прежде чем устанавливать сервер IBM Spectrum Protect в операционной системе Linux on Power Systems (с прямым порядком байтов), ознакомьтесь с требованиями к аппаратному и программному обеспечению.

Требования к аппаратному и программному обеспечению для установки сервера IBM Spectrum Protect

Самую последнюю информацию о требованиях к системе IBM Spectrum Protect смотрите в техническом замечании 1243309.

В Таблица 10 на стр. 56 приводятся минимальные требования к аппаратному обеспечению вашей системы.

Таблица 10. Требования к аппаратным средствам

Тип аппаратуры	Требования к аппаратным средствам
Общее	Сервер Linux on Power Systems (с прямым порядком байтов) в системе IBM, например, в системе, указанной на веб-сайте Linux on IBM Power Systems.

Таблица 10. Требования к аппаратным средствам (продолжение)

Тип аппаратуры	Требования к аппаратным средствам
Дисковое пространство	Следующий минимальный объем дискового пространства: • 4.3 ГБ для каталога установки • 2.5 ГБ для каталога `/var` • 4 ГБ для каталога `/tmp` • 128 МБ для домашнего каталога для пользователя root • 2 ГБ для области совместно используемых ресурсов Если возникнет проблема и потребуется какая-либо диагностика, оптимальным является, чтобы в системе было доступно временное или другое пространство для журнала захвата данных первой ошибки (first failure data capture, FFDC) или для другого временного использования, например, для сбора журналов трассировки. Для базы данных и файлов журналов дополнительно требуется значительный объем дискового пространства. Размер базы данных зависит от количества клиентских файлов, которые необходимо хранить, и метода, с помощью которого сервер управляет ими. Объем пространства активного журнала по умолчанию равен 16 ГБ; это необходимый минимум для большинства рабочих нагрузок и конфигураций. При создании активного журнала нужно, по крайней мере, 64 ГБ для выполнения репликации. Если используются и репликация, и дедупликация данных, создайте активный журнал, размер которого будет равен 128 ГБ. Выделите для архивного журнала, как минимум, в три раза больший объем пространства, чем для активного журнала по умолчанию (48 ГБ). Если вы используете дедупликацию данных или ожидаете высокий уровень рабочей нагрузки на клиент, убедитесь, что у вас достаточно ресурсов. Чтобы обеспечить оптимальную производительность и эффективность ввода-вывода, задайте, как минимум, два контейнера с одинаковым размером или с одинаковыми номерами Logical Unit Number (LUN), которые будут использоваться базой данных. Кроме того, для каждого активного журнала и архивного журнала нужен свой собственный контейнер или LUN. Обязательно ознакомьтесь с более подробной информацией о дисковом пространстве в разделе “Планирование емкости” на стр. 62.
Память	• 16 ГБ для стандартных операций сервера без дедупликации данных и репликации узлов • 24 ГБ для дедупликации данных или репликации узлов • 32 ГБ для репликации узлов с дедупликацией данных Более конкретные требования к памяти для более крупных баз данных и большей возможности поглощения смотрите в документе Таблица настройки памяти сервера IBM Spectrum Protect. Особые требования к памяти, когда используется дедупликация данных, смотрите в документе IBM Spectrum Protect Blueprint для вашей операционной системы.

Требования к программному обеспечению

В Таблица 11 на стр. 58 приводятся минимальные требования к программному обеспечению вашей системы.

Таблица 11. Требования к программному обеспечению

Тип программного обеспечения	Минимальные требования к программному обеспечению
Операционная система	Серверу IBM Spectrum Protect в Linux on Power Systems (с прямым порядком байт) требуется одна из следующих операционных систем: • Red Hat Enterprise Linux 8.1 или новее • Red Hat Enterprise Linux 7.6 или новее • SUSE Linux Enterprise Server 15, SP1 или новее • SUSE Linux Enterprise Server 12, SP4 или новее **Ограничение:** Функция обнаружения сети хранения данных (storage area network, SAN) не поддерживается. • Ubuntu Server LTS версии 16.04.2 или 18.04. В случае ленточного хранения минимальной версией Ubuntu Server LTS является версия 18.04.
Библиотеки	Библиотеки GNU C версии 2.4-31.30 и новее. • libaio.so.1 (32- и 64-разрядные пакеты) • libnuma.so.1 Чтобы определить, установлен ли SELinux и включен ли режим принудительного применения, выполните одно из следующих действий: • Проверьте файл `/etc/sysconfig/selinux`. • Введите команду операционной системы **`sestatus`**. • Проверьте наличие в файле `/var/log/messages` сообщений SELinux. **Ограничение:** Для установок и обновления IBM Spectrum Protect нужно отключить SELinux. Чтобы отключить SELinux, выполните одну из следующих задач: • Чтобы задать режим permissive, введите команду `setenforce 0` от имени суперпользователя. • Измените файл `/etc/sysconfig/selinux` и перезапустите компьютер.
Протокол связи	• TCP/IP V4 или V7, входящий в стандартный комплект поставки Linux • Протокол совместно используемой памяти (Shared Memory)
Обработка	Должен быть включен асинхронный ввод-вывод. В системе Linux с ядром версии 2.6 и новее для включения асинхронного ввода-вывода установите библиотеку libaio.
Другое программное обеспечение	• Оболочка Korn (ksh) • Для аутентификации пользователей IBM Spectrum Protect посредством сервера Lightweight Directory Access Protocol нужно использовать один из следующих серверов каталогов: – Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2, Windows Server 2016) – IBM Security Directory Server V6.3 – IBM Security Directory Server V6.4

Ограничение: Неформатированные логические тома не поддерживаются.

Совместимость сервера IBM Spectrum Protect с другими продуктами IBM Db2 в системе

При определенных ограничениях на одном компьютере с сервером IBM Spectrum Protect можно установить другие продукты, которые тоже внедряют и используют Db2.

Если вы хотите установить и использовать другие продукты, которые используют продукт Db2, на одном компьютере с сервером IBM Spectrum Protect, убедитесь, что выполняются следующие условия:

Таблица 12. Совместимость сервера IBM Spectrum Protect с другими продуктами Db2 в системе

Критерий	**Инструкции**
Уровень версии	Другие продукты, использующие Db2, должны использовать Db2 версии 9 или новее. Продукты Db2 включают в себя поддержку инкапсуляции и разделения продуктов, начиная с версии 9. Начиная с этой версии, можно запускать несколько копий продуктов Db2 с разными уровнями кода в одной системе. Чтобы узнать об этом подробнее, смотрите информацию о нескольких копиях по адресу: Информация о продукте Db2.
ID и каталоги пользователей	Убедитесь, что ID пользователей, ID изолированных пользователей, положение установки, другие каталоги и связанная информация не используются одновременно в нескольких установках Db2. Ваши спецификации должны отличаться от тех ID и положений, которые использовались для установки и конфигурирования сервера IBM Spectrum Protect. Если вы сконфигурировали сервер при помощи мастера **dsmicfgx**, это будут значения, введенные вами во время работы с мастером. Если вы использовали метод конфигурирования вручную, вспомните, какие значения вы использовали для сервера при выполнении этих процедур (если это потребуется).

Таблица 12. Совместимость сервера IBM Spectrum Protect с другими продуктами Db2 в системе (продолжение)

Критерий	Инструкции
Выделение ресурсов	Оцените ресурсы и возможности системы, сопоставив их как с требованиями для сервера IBM Spectrum Protect, так и для других программ, которые используют продукт Db2. Чтобы обеспечить достаточно ресурсов для других приложений Db2, нужно изменить параметры сервера IBM Spectrum Protect, так чтобы сервер использовал меньше памяти и ресурсов. Аналогичным образом, если рабочие нагрузки для других приложений Db2 таковы, что между этими приложениями и сервером IBM Spectrum Protect возникает конфликт доступа к ресурсам процессора или памяти, это может отрицательно сказаться на производительности сервера при обработке ожидаемой рабочей нагрузке клиента или при выполнении других серверных операций. Чтобы разделить ресурсы и обеспечить больше возможностей настройки и распределения ресурсов процессора и памяти и других системных ресурсов между несколькими приложениями, рассмотрите возможность использования логических разделов (Logical Partition - LPAR), разделов рабочей нагрузки (Workload Partition - WPAR) или иной поддержки виртуальных рабочих станций. Например, запускайте программу Db2 в ее собственной виртуальной системе.

IBM Installation Manager

IBM Spectrum Protect использует IBM Installation Manager - программу установки, которая может использовать удаленные или локальные репозитории программ для установки или обновления многих продуктов IBM.

Если обязательная версия IBM Installation Manager еще не установлена, то она автоматически устанавливается или обновляется при установке IBM Spectrum Protect. Она должна остаться установленной на компьютере, чтобы позже можно было обновить или деинсталлировать IBM Spectrum Protect.

Ниже приведены объяснения некоторых терминов, используемых в IBM Installation Manager:

Предложение
Устанавливаемый модуль программного продукта.

Предложение IBM Spectrum Protect содержит все носители, которые требуются IBM Installation Manager для установки IBM Spectrum Protect.

Пакет
Группа программных компонентов, необходимых для установки предложения.

Пакет IBM Spectrum Protect включает в себя следующие компоненты:

- Программа установки IBM Installation Manager
- Предложение IBM Spectrum Protect

Группа пакетов
Набор пакетов, использующих общий родительский каталог.

Группа пакетов по умолчанию для пакета IBM Spectrum Protect - `IBM Installation Manager`.

Репозиторий
Удаленная или локальная область хранения данных и других ресурсов программы.

Пакет IBM Spectrum Protect хранится в репозитории в IBM Fix Central.

Каталог общих ресурсов
Каталог, содержащий файлы или подключаемые модули программ, которые совместно используются пакетами.

IBM Installation Manager хранит в каталоге общих ресурсов связанные с установкой файлы, включая файлы, используемые для отката к предыдущей версии IBM Spectrum Protect.

Контрольные списки для планирования сведений о сервере

Контрольные списки помогут вам спланировать объем и расположение пространства хранения, необходимого серверу IBM Spectrum Protect. Их можно использовать также для сохранения трассировки имен и ID пользователей.

Элемент	Необходимое пространство	Число каталогов	Положение каталогов
База данных			
Активный журнал			
Архивный журнал			
Необязательно: Зеркальная копия активного журнала			
Необязательно: Вторичный архивный журнал (резервный каталог для архивного журнала)			

Элемент	Имена и ID пользователей	Расположение
ID пользователя экземпляра для сервера, то есть ID, который использовался для запуска и работы сервера IBM Spectrum Protect		

Элемент	Имена и ID пользователей	Расположение
Домашний каталог для сервера, то есть каталог, содержащий ID пользователя экземпляра		
Имя экземпляра базы данных		
Каталог экземпляра для сервера, представляющий собой каталог с файлами, связанными именно с данным экземпляром сервера (файл серверных опций и другие файлы, связанные с сервером)		
Имя сервера; для каждого сервера используйте уникальное имя		

Планирование емкости

Планирование емкости для IBM Spectrum Protect включает в себя управление такими ресурсами, как база данных, журнал восстановления и совместно используемая область ресурсов.

Прежде чем начать

Для максимального увеличения ресурсов как части планирования емкости необходимо оценить требования к пространству для базы данных и журнала восстановления. В области совместно используемых ресурсов должно быть достаточно пространства для каждой установки или обновления.

Оценка необходимого объема пространства для базы данных

Оценить необходимое для базы данных пространство можно, исходя из максимально допустимого числа файлов, одновременного находящихся в системе хранения сервера, или на основе емкости пула хранения.

Об этой задаче

В качестве начального объема пространства базы данных можно порекомендовать использовать не менее 25 ГБ. Доступ к пространству файловой системы предоставляется должным образом. Размер базы данных 25 ГБ достаточен для среды тестирования или среды, включающей только менеджер библиотек. Для производственного сервера с поддержкой клиентских рабочих нагрузок размер базы данных должен быть больше. Если вы используете дисковые пулы хранения с произвольным доступом (DISK), потребуется дополнительное пространство хранения баз данных и журналов для пулов хранения с последовательным доступом.

Максимальный размер базы данных IBM Spectrum Protect - 8 ТБ.

Информацию об оценке размера базы данных в производственной среде на основе числа файлов и размера пула хранения смотрите в темах ниже.

Оценка требований к пространству базы данных на основе числа файлов

Если возможно оценить максимальное количество файлов, которые будут одновременно находиться в системе хранения сервера, это число можно использовать для оценки требований к пространству базы данных.

Об этой задаче

Для оценки требований к объему пространства на основе максимального числа файлов в системе хранения сервера используйте следующие рекомендации:

- 600 - 1000 байт на каждую хранимую версию файла, включая резервные копии образов.

  Ограничение: Сюда не входит пространство, используемое во время дедупликации данных.
- 100 - 200 байт на каждый кэшированный файл, файл пула хранения копий, файл пула активных данных и дедуплицированный файл.
- Дополнительное пространство требуется для оптимизации базы данных в части поддержки переменных схем доступа к данным и внутренней обработки данных на сервере. Объем дополнительного пространства равен 50% оцененного размера памяти для хранения файловых объектов.

В следующем примере для единственного клиента вычисления основываются на максимальных значениях из предыдущих инструкций. В примерах не учитывается возможное использование объединения файлов. В общем случае объединение файлов сокращает объем требуемого пространства базы данных. Объединение файлов не затрагивает перенесенные файлы.

Процедура

1. Вычислите число версий файлов. Чтобы получить число версий файлов, сложите следующие значения:
   a) Вычислите число резервных копий файлов.
   Например, одновременно может существовать до 500 000 резервных копий клиентских файлов. В этом примере политики хранения требуют, чтобы хранилось до трех резервных копий каждого файла:

   ```
   500 000 файлов * 3 копии = 1 500 000 файлов
   ```

   b) Вычислите количество архивных файлов.
   Например, до 100 000 клиентских файлов могут быть архивными копиями.

   c) Вычислите количество перенесенных файлов.
   Например, до 200 000 клиентских файлов могут быть перемещены с клиентских рабочих станций.

   Если для каждого файла требуется 1000 байт, то общий объем требуемого для принадлежащих клиентам файлов пространства базы данных - 1,8 ГБ.

   ```
   (1 500 000 + 100 000 + 200 000) * 1000 = 1,8 ГБ
   ```

2. Вычислите число кэшированных файлов, файлов пула хранения копий, файлов пула активных данных и дедуплицированных файлов:
   a) Вычислите количество кэшированных копий.
   Например, кэширование разрешено в дисковом пуле хранения размером 5 ГБ. Верхний порог переноса пула равен 90%, а нижний - 70%. Таким образом, 20% дискового пула, то есть 1 ГБ, будет занято кэшированными файлами.

   Если средний размер файла около 10 КБ, в кэше в любой момент времени находится около 100000 файлов:

   ```
   100 000 файлов * 200
   байт = 19 МБ
   ```

   b) Вычислите количество файлов пула хранения копий.
   Для всех основных пулов памяти создается резервная копия:

   ```
   (1 500 000 + 100 000 + 200 000) * 200 байт = 343 МБ
   ```

   c) Вычислите количество активных файлов пула хранения.

Все данные активных резервных копий клиента в первичных пулах хранения копируются в пул хранения активных данных. Допустим, что 500 000 версий 1 500 000 резервных копий файлов в основном пуле являются активными:

```
500 000 * 200 байт = 95 МБ
```

d) Вычислите количество дедуплицированных данных.
Допустим, что пул хранения данных, подвергнутых дедупликации, содержит 50000 файлов:

```
50 000 * 200 байт = 10 МБ
```

На основании этих вычислений для клиентских кэшированных файлов, файлов пула хранения копий, файлов пула активных данных и дедуплицированных файлов требуется примерно 0,5 ГБ дополнительного пространства базы данных.

3. Вычислите объем дополнительного пространства, требуемый для оптимизации базы данных. Для обеспечения оптимального доступа к данным и управления сервером требуется дополнительное пространство базы данных. Объем дополнительного пространства базы данных равен 50% общего пространства, необходимого для хранения файловых объектов.

```
(1,8 + 0,5) * 50% = 1,2 ГБ
```

4. Вычислите общий объем пространства базы данных, требуемый для этого клиента. Общий объем составит примерно 3,5 ГБ:

```
1,8 + 0,5 + 1,2 = 3,5 ГБ
```

5. Вычислите общий объем пространства базы данных, требуемый для всех клиентов.
Если предыдущие оценки приведены для типичного клиента и у вас 500 таких клиентов, то можно использовать для примера следующую оценку общего объема пространства базы данных, требуемого для всех клиентов:

```
500 * 3,5 = 1,7 ТБ
```

Результаты

Совет: В приведенных выше примерах результаты представляют собой примерные оценки. Фактический размер базы данных может отличаться от ожидаемого из-за таких факторов, как число каталогов и длина полных имен файлов. Рекомендуется периодически производить мониторинг базы данных и корректировать ее размер, если потребуется.

Дальнейшие действия

При обычных операциях серверу IBM Spectrum Protect может потребоваться временное пространство баз данных. Это пространство необходимо для следующих задач:

- Сохранять результаты сортировки или упорядочивания, которые еще не сохранены и не оптимизированы непосредственно в базе данных. Эти результаты временно сохраняются в базе данных для обработки.
- Предоставлять административный доступ к базе данных одним из следующих способов:
  - Через клиент Open Database Connectivity (ODBC) Db2
  - Через клиент Oracle Java Database Connectivity (JDBC)
  - Из командной строки клиента администрирования на сервер с помощью Structured Query Language (SQL)

Используйте дополнительные 50 ГБ временного пространства на каждые 500 ГБ пространства для файловых объектов и оптимизации. Смотрите инструкции в следующей таблице. В примере, использованном в предыдущем шаге, для файловых объектов и оптимизации для 500 клиентов требуется общий объем пространства базы данных 1,7 ТБ. На основании этих оценок еще около

200 ГБ требуется для временного пространства. Суммарный объем требуемого пространства базы данных составляет 1,9 ТБ.

Размер базы данных	Минимальные потребности временного пространства
< 500 ГБ	50 ГБ
≥ 500 ГБ и < 1 ТБ	100 ГБ
≥ 1 ТБ и < 1,5 ТБ	150 ГБ
≥ 1,5 и < 2 ТБ	200 ГБ
≥ 2 и < 3 ТБ	250 - 300 ГБ
≥ 3 и < 4 ТБ	350 - 400 ГБ

Оценка требований к пространству базы данных на основе мощности пула хранения

Чтобы оценить требования к пространству базы данных на основе мощности пула хранения, используйте коэффициент 1 - 5%. Например, если вам требуется мощность пула хранения в 200 ТБ, размер базы данных составит примерно 2 - 10 ТБ. Как общее правило, сделайте вашу базу данных настолько большой, насколько это возможно, чтобы предотвратить недостаток памяти. Если в пространстве базы данных не хватит памяти, может произойти сбой операций сервера и операций сохранения, выполняемых клиентом.

Менеджер баз данных и временное пространство

Менеджер баз данных сервера IBM Spectrum Protect выделяет системную память и дисковое пространство для базы данных и управляет ими. Объем нужного пространства базы данных зависит от объема доступной памяти системы и рабочей нагрузки сервера.

Менеджер баз данных сортирует данные в определенном порядке, как в операторе SQL, который вводится для запроса данных. В зависимости от рабочей нагрузки на сервере, если объем данных больше, чем может обрабатывать менеджер баз данных, эти упорядоченные данные размещаются во временном дисковом пространстве. Данные располагаются во временном дисковом пространстве, когда уже существует большой набор результатов. Менеджер баз данных динамически управляет памятью, используемой при размещении данных во временном дисковом пространстве.

Например, большой объем результатов может возникнуть при обработке устаревания данных. Если памяти системы недостаточно для хранения набора результатов, некоторые данные размещаются во временной дисковом пространстве. Если во время обработки устаревания выбран чрезмерно большой узел или файловое пространство, то менеджер баз данных не сможет отсортировать данные в памяти. Для сортировки данных менеджеру баз данных понадобится временное пространство.

Чтобы запустить операции базы данных, рассмотрите возможность добавления пространства базы данных для следующих сценариев:

- У базы данных маленький объем пространства, и операции сервера, которым требуется временное пространство, используют оставшуюся незанятую память.
- Файловые пространства велики, или для них назначена политика, которая создает много версий файлов.
- Сервер IBM Spectrum Protect должен быть запущен с ограниченным объемом памяти. Для запуска своих операций база данных использует главную память сервера IBM Spectrum Protect. Однако если памяти недостаточно, сервер IBM Spectrum Protect выделяет для базы данных временное пространство на диске. Например, если доступно 10 ГБ памяти, а для операций базы данных требуется 12 ГБ, база данных использует временное пространство.

- При внедрении сервера IBM Spectrum Protect появится сообщение об ошибке недостаток памяти базы данных. Отслеживайте в активном журнале сервера сообщения, относящиеся к пространству баз данных.

Важное замечание: Не изменяйте программу Db2, устанавливаемую вместе с пакетами установки и пакетами исправлений IBM Spectrum Protect. Не устанавливайте другую версию, выпуск или пакет исправлений и не производите обновление до другой версии, выпуска или пакета исправлений программы Db2, чтобы не повредить базу данных.

Требования к пространству журнала восстановления

В IBM Spectrum Protect термин *журнал восстановления* включает в себя активных журнал, архивный журнал, зеркальную копию активного журнала и архивный журнал восстановления при отказе. Требуемый объем пространства для журнала восстановления зависит от различных факторов, например, от интенсивности операций клиента на сервере.

Пространство активных и архивных журналов

Оценивая необходимый размер памяти для активного и архивного журналов, включите несколько дополнительных страниц на случай непредвиденных обстоятельств, например, случайных тяжелых рабочих нагрузок и восстановления после сбоя.

Максимальный размер активного журнала для серверов IBM Spectrum Protect версии 7.1 и новее должен составлять 512 ГБ. Размер архивного журнала ограничен размером файловой системы, в которой он установлен.

Учитывайте следующие общие рекомендации для оценки размера активного журнала:

- Рекомендуемый начальный размер активного журнала - 16 ГБ.
- Убедитесь, что размер активного журнала достаточен, по крайней мере, для тех текущих операций, которые обычно обрабатываются сервером. В качестве меры предосторожности попытайтесь учесть наибольший объем работы, которую сервер может выполнять единовременно. Обеспечьте для активного журнала некоторый дополнительный объем пространства, которое может использоваться при необходимости. Предусмотрите 20% дополнительного пространства.
- Отслеживайте используемое и доступное пространство активного журнала. При необходимости подстраивайте размер активного журнала в зависимости от таких факторов, как активность клиентов и уровень операций сервера.
- Убедитесь, что размер каталога, в котором содержится активный журнал, не меньше размера самого журнала. Если каталог больше по размеру, чем активный журнал, при необходимости он может использоваться для обработки аварийного восстановления.
- Убедитесь, что в файловой системе, которая содержит каталог активного журнала, есть по крайней мере 8 ГБ свободного места для требований временных перемещений журналов.

Рекомендуемый начальный размер архивного журнала - 48 ГБ.

Каталог архивного журнала должен быть достаточно большим, чтобы в нем уместились файлы журнала, сгенерированные с момента последнего полного резервного копирования. Например, если вы производите резервное копирование базы данных ежедневно, каталог архивного журнала должен быть достаточно большим, чтобы в нем уместились файлы журнала для всех операций клиентов в течение 24 часов. Чтобы освободить пространство, при полном резервном копировании базы данных сервер удаляет устаревшие файлы архивного журнала. Если каталог архивного журнала переполняется, а каталог резервного архивного журнала не существует, файлы журнала остаются в каталоге активного журнала. Это условие может привести к остановке сервера в связи с переполнением каталога активного журнала. При повторном запуске сервера часть используемого для активного журнала пространства освобождается.

После установки сервера вы можете отслеживать использование архивного журнала и пространство каталога архивного журнала. Если каталог архивного журнала переполняется, то это может привести к следующим проблемам:

- Сервер не сможет провести полное резервное копирование базы данных. Исследуйте и разрешите эту проблему.
- Другие приложения, выполняют запись в каталог архивного журнала, уменьшая объем доступного для архивного журнала пространства. Не используйте пространство архивного журнала для других приложений, в том числе для других серверов IBM Spectrum Protect. Убедитесь, что у каждого сервера существует отдельное положение хранения, которым владеет и управляет данный сервер.

Пример: оценка размера активного и архивного журналов для основных операций сохранения данных клиентами

Основные операции сохранения данных клиентами включают в себя резервное копирование, архивирование и управление пространством. Пространство журналов должно быть достаточно большим, чтобы обрабатывать все выполняемые одновременно операции сохранения.

Чтобы определить размеры активных и архивных журналов для основных операций сохранения, выполняемых клиентами, используйте следующую формулу:

```
число клиентов  x  число файлов, сохраненных в течение каждой транзакции
  x  размер пространства журнала, необходимый для каждого файла
```

Такое вычисление использовано в примере в следующей таблице.

Таблица 13. Основные операции сохранения данных клиентами

Элемент	Значения примера	Описание
Максимальное число клиентских узлов, в которых одновременно выполняется резервное копирование, архивирование и перенос данных в любое время	300	Число клиентских узлов, в которых производится резервное копирование, архивирование и перенос данных каждую ночь.
Количество файлов, сохраняемых за каждую транзакцию	4096	Значение опции сервера TXNGROUPMAX по умолчанию - 4096.
Размер пространства журналов, необходимый для каждого файла	3053 байта	Значение 3053 байта для каждого файла в транзакции представляет количество байт в журнале, необходимое для резервного копирования файлов от клиента Windows, где длина имен файлов - от 12 до 120 байт. Это значение основывается на результатах тестов, выполненных в лабораторных условиях. Эти тесты включали в себя клиенты резервного копирования и архивирования, выполнявшие операции резервного копирования в дисковый пул хранения с произвольным доступом (DISK). Пулы DISK приводят к большему размеру журналов, чем пулы хранения последовательного доступа. Применяйте в расчетах значения, большие 3053 байт, если длина имен сохраняемых файлов - больше, чем от 12 до 120 байт.

Таблица 13. Основные операции сохранения данных клиентами (продолжение)

Элемент	Значения примера	Описание

Активный журнал: Рекомендуемый размер	19,5 ГБ [1]	Используйте следующую формулу для вычисления размера активного журнала. Один гигабайт равен 1 073 741 824 байт.
		`(300 клиентов x 4096 сохраняемых за каждую транзакцию файлов x 3053 байта на каждый файл) ÷ 1 073 741 824 байт = 3,5 ГБ`
		Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
		`3,5 + 16 = 19,5 ГБ`

Архивный журнал: Рекомендуемый размер	58,5 ГБ [1]	Из-за требования возможности сохранения архивных журналов за три цикла резервного копирования базы данных сервера умножьте этот оценочный размер активного журнала на 3, чтобы оценить суммарные требования к размеру архивного журнала.
		`3,5 x 3 = 10,5 ГБ`
		Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
		`10,5 + 48 = 58,5 ГБ`

[1] Значения примера в этой таблице используются только, чтобы показать, как вычисляются размеры активных журналов и архивных журналов. В производственной среде, где не используется дедупликация, предлагаемый минимальный размер активного журнала - 16 ГБ. Предлагаемый минимальный размер архивного журнала в производственной среде, где не используется дедупликация, составляет 48 ГБ. Если при подстановке в приведенные оценки значений для вашей среды получатся результаты, превышающие 16 ГБ и 48 ГБ, используйте большие величины для оценки размера активного и архивного журнала.

Отслеживайте свои журналы и при необходимости настраивайте их размеры.

Пример: оценка размеров активных и неактивных журналов для клиентов, использующих несколько сеансов

Если для опции клиента RESOURCEUTILIZATION задано большее значение, чем по умолчанию, из-за одновременности выполнения увеличивается рабочая нагрузка на сервер.

Чтобы определить размеры активных и архивных журналов, когда клиенты используют несколько сеансов, примените следующую формулу:

```
число клиентов  x  число сеансов для каждого клиента  x  число файлов, сохраненных
  в течение каждой транзакции  x  объем памяти журнала, необходимой для каждого файла
```

Такое вычисление использовано в примере в следующей таблице.

Таблица 14. Несколько сеансов клиента

Элемент	Значения примера		Описание
Максимальное число клиентских узлов, в которых одновременно выполняется резервное копирование, архивирование и перенос данных в любое время	300	1000	Число клиентских узлов, в которых производится резервное копирование, архивирование и перенос данных каждую ночь.
Возможных сеансов для каждого клиента	3	3	Параметр опции клиента RESOURCEUTILIZATION больше, чем значение по умолчанию. Каждый сеанс клиента запускает параллельно до трех сеансов.
Количество файлов, сохраняемых за каждую транзакцию	4096	4096	Значение опции сервера TXNGROUPMAX по умолчанию - 4096.
Размер пространства журналов, необходимый для каждого файла	3053	3053	Значение 3053 байта для каждого файла в транзакции представляет количество байт в журнале, необходимое для резервного копирования файлов от клиента Windows, где длина имен файлов - от 12 до 120 байт. Это значение основывается на результатах тестов, выполненных в лабораторных условиях. Эти тесты включали в себя клиенты резервного копирования и архивирования, выполнявшие операции резервного копирования в дисковый пул хранения с произвольным доступом (DISK). Пулы DISK приводят к большему размеру журналов, чем пулы хранения последовательного доступа. Применяйте в расчетах значения, большие 3053 байт, если длина имен сохраняемых файлов - больше, чем от 12 до 120 байт.

Активный журнал: Рекомендуемый размер	26,5 ГБ [1]	51 ГБ [1]	Следующие вычисления проведены для 300 клиентов: Один гигабайт равен 1 073 741 824 байт.
			
			`(300 клиентов x 3 сеанса на каждого клиента x 4096 сохраняемых за каждую транзакцию файлов x 3053 байта на каждый файл) ÷ 1 073 741 824 = 10,5 ГБ`
			
			Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
			
			`10,5 + 16 = 26,5 ГБ`
			
			Следующие вычисления проведены для 1000 клиентов: Один гигабайт равен 1 073 741 824 байт.
			
			`(1000 клиентов x 3 сеанса на каждого клиента x 4096 сохраняемых за каждую транзакцию файлов x 3053 байта на каждый файл) ÷ 1 073 741 824 = 35 ГБ`
			
			Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
			
			`35 + 16 = 51 ГБ`

Таблица 14. Несколько сеансов клиента (продолжение)

Элемент	Значения примера		Описание

Архивный журнал: Рекомендуемый размер	79,5 ГБ [1]	153 ГБ [1]	Из-за требования возможности сохранения архивных журналов за три цикла резервного копирования базы данных сервера умножьте этот оценочный размер активного журнала на 3, чтобы оценить суммарные требования к размеру архивного журнала:
			`10,5 x 3 = 31,5 ГБ`
			`35 x 3 = 105 ГБ`
			Увеличим эти размеры на рекомендуемый начальный размер 48 ГБ:
			`31,5 + 48 = 79,5 ГБ`
			`105 + 48 = 153 ГБ`

[1] Значения примера в этой таблице используются только, чтобы показать, как вычисляются размеры активных журналов и архивных журналов. В производственной среде, где не используется дедупликация, предлагаемый минимальный размер активного журнала - 16 ГБ. Предлагаемый минимальный размер архивного журнала в производственной среде, где не используется дедупликация, составляет 48 ГБ. Если при подстановке в приведенные оценки значений для вашей среды получатся результаты, превышающие 16 ГБ и 48 ГБ, используйте большие величины для оценки размера активного и архивного журнала.

Отслеживайте ваш активный журнал и при необходимости настраивайте его размер.

Пример: оценка размера активного и архивного журналов для операций одновременной записи

Если операции резервного копирования клиентов используют пулы хранения, которые сконфигурированы для одновременной записи, увеличивается объем пространства журнала, требуемого для каждого файла.

Пространство журнала, требуемое для каждого файла, увеличивается примерно на 200 байт на каждый пул хранения копий, который используется для операции одновременной записи. В примере в следующей таблице данные сохраняются в двух пулах хранения копий в дополнение к первичному пулу хранения. Оценочный размер журнала увеличивается на 400 байт для каждого файла. Если использовать рекомендованное значение памяти журнала для каждого файла (3053 байта), полный объем составит 3453 байта.

Такое вычисление использовано в примере в следующей таблице.

Таблица 15. Одновременные операции записи

Элемент	Значения примера	Описание
Максимальное число клиентских узлов, в которых одновременно выполняется резервное копирование, архивирование и перенос данных в любое время	300	Число клиентских узлов, в которых производится резервное копирование, архивирование и перенос данных каждую ночь.
Количество файлов, сохраняемых за каждую транзакцию	4096	Значение опции сервера TXNGROUPMAX по умолчанию - 4096.

Таблица 15. Одновременные операции записи (продолжение)

Элемент	Значения примера	Описание
Размер пространства журналов, необходимый для каждого файла	3453 байта	3053 байта на каждый файл плюс 200 байт на каждый пул хранения копий. Значение 3053 байта для каждого файла в транзакции представляет количество байт в журнале, необходимое для резервного копирования файлов от клиента Windows, где длина имен файлов - от 12 до 120 байт. Это значение основывается на результатах тестов, выполненных в лабораторных условиях. Эти тесты включали в себя клиенты резервного копирования и архивирования, выполнявшие операции резервного копирования в дисковый пул хранения с произвольным доступом (DISK). Пулы DISK приводят к большему размеру журналов, чем пулы хранения последовательного доступа. Применяйте в расчетах значения, большие 3053 байт, если длина имен сохраняемых файлов - больше, чем от 12 до 120 байт.

Активный журнал: Рекомендуемый размер	20 ГБ [1]	Используйте следующую формулу для вычисления размера активного журнала. Один гигабайт равен 1 073 741 824 байт.
		
		`(300 клиентов x 4096 сохраняемых за каждую транзакцию файлов x 3453 байта на каждый файл) ÷ 1 073 741 824 байт = 4,0 ГБ`
		
		Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
		
		`4 + 16 = 20 ГБ`

Архивный журнал: Рекомендуемый размер	60 ГБ [1]	Из-за требования возможности сохранения архивных журналов за три цикла резервного копирования базы данных сервера умножьте этот оценочный размер активного журнала на 3, чтобы оценить требования к размеру архивного журнала:
		
		`4 ГБ x 3 = 12 ГБ`
		
		Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
		
		`12 + 48 = 60 ГБ`

[1] Значения примера в этой таблице используются только, чтобы показать, как вычисляются размеры активных журналов и архивных журналов. В производственной среде, где не используется дедупликация, предлагаемый минимальный размер активного журнала - 16 ГБ. Предлагаемый минимальный размер архивного журнала в производственной среде, где не используется дедупликация, составляет 48 ГБ. Если при подстановке в приведенные оценки значений для вашей среды получатся результаты, превышающие 16 ГБ и 48 ГБ, используйте большие величины для оценки размера активного и архивного журнала.

Отслеживайте свои журналы и при необходимости настраивайте их размеры.

Пример: оценка размера активных и архивных журналов для основных операций сохранения данных клиентами и операций сервера

Перемещения данных в системе хранения сервера, процессы идентификации для дедупликации, освобождение памяти и обработка устаревших данных могут происходить одновременно с операциями сохранения данных клиентами. Задачи администрирования, такие как административные команды и запросы SQL от клиентов администрирования, могут также выполняться одновременно с операциями сохранения данных клиентами. Операции сервера и административные задачи, выполняемые одновременно, могут увеличить требуемый объем памяти активного журнала.

Например, перемещение данных из дискового пула хранения с произвольным доступом (DISK) в дисковый пул хранения с последовательным доступом (FILE) использует примерно 110 байт памяти журнала на каждый перемещаемый файл. Допустим, например, что у вас есть 300 клиентов архивирования и резервного копирования, и каждый из них проводит резервное копирование 100 000 файлов каждую ночь. Файлы изначально хранятся в пуле хранения DISK, а затем переносятся в пул хранения FILE. Чтобы оценить объем памяти активного журнала, требуемой для этого перемещения данных, воспользуемся следующим вычислением. Число клиентов в формуле представляет собой максимальное число клиентских узлов, в которых одновременно выполняется резервное копирование, архивирование и перенос данных в любое время.

```
300 клиентов  x 100 000 файлов на каждого клиента  x  110 байт =  3,1 ГБ
```

Добавьте это значение к оценке размера активного журнала, полученной для основных операций сохранения данных клиентами.

Пример: оценка размера активных и архивных журналов в условиях сильной неоднородности

Проблемы с недостатком памяти для активного журнала могут возникнуть в том случае, если есть много быстро заканчивающихся транзакций и несколько транзакций, которым требуется гораздо больше времени для завершения. Типичная ситуация возникает, когда активны многие сеансы резервного копирования рабочих станций или файл-серверов и одновременно активны несколько сеансов резервного копирования очень больших баз данных. Если такая ситуация применима к вашей среде, вам может потребоваться увеличить размер памяти активного журнала, чтобы работа завершилась успешно.

Пример: оценка размеров архивных журналов с полными резервными копиями базы данных

Сервер IBM Spectrum Protect удаляет ненужные файлы из архивного журнала только после полного резервного копирования базы данных. Следовательно, при оценке требуемой для архивного журнала памяти необходимо учитывать и периодичность полного резервного копирования базы данных.

Например, если полное резервное копирование базы данных производится раз в неделю, размер архивного журнала должен быть достаточным, чтобы содержать всю информацию за неделю в архивном журнале.

Различие в размерах архивного журнала для ежедневных и полных резервных копирований базы данных показано в примере в следующей таблице.

Таблица 16. Полное резервное копирование базы данных

Элемент	Значения примера	Описание
Максимальное число клиентских узлов, в которых одновременно выполняется резервное копирование, архивирование и перенос данных в любое время	300	Число клиентских узлов, в которых производится резервное копирование, архивирование и перенос данных каждую ночь.

Таблица 16. Полное резервное копирование базы данных (продолжение)

Элемент	Значения примера	Описание
Количество файлов, сохраняемых за каждую транзакцию	4096	Значение опции сервера TXNGROUPMAX по умолчанию - 4096.
Размер пространства журналов, необходимый для каждого файла	3453 байта	3053 байт на каждый файл плюс 200 байт на каждый пул хранения копий. Значение 3053 байта для каждого файла в транзакции представляет количество байт в журнале, необходимое для резервного копирования файлов от клиента Windows, где длина имен файлов - от 12 до 120 байт. Это значение основывается на результатах тестов, выполненных в лабораторных условиях. Эти тесты включали в себя клиенты резервного копирования и архивирования, выполнявшие операции резервного копирования в дисковый пул хранения с произвольным доступом (DISK). Пулы DISK приводят к большему размеру журналов, чем пулы хранения последовательного доступа. Применяйте в расчетах значения, большие 3053 байт, если длина имен сохраняемых файлов - больше, чем от 12 до 120 байт.

Активный журнал: Рекомендуемый размер	20 ГБ [1]	Используйте следующую формулу для вычисления размера активного журнала. Один гигабайт равен 1 073 741 824 байт.
		`(300 клиентов x 4096 файлов на транзакцию x 3453 байт на файл) ÷ 1 073 741 824 байт = 4,0 ГБ`
		Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
		`4 + 16 = 20 ГБ`

Архивный журнал: Рекомендованный размер при ежедневном полном резервном копировании базы данных	60 ГБ [1]	Из-за требования возможности сохранения архивных журналов за три цикла резервного копирования базы данных сервера умножьте этот оценочный размер активного журнала на 3, чтобы оценить суммарные требования к размеру архивного журнала:
		`4 ГБ x 3 = 12 ГБ`
		Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
		`12 + 48 = 60 ГБ`

Таблица 16. Полное резервное копирование базы данных (продолжение)

Элемент	Значения примера	Описание

Архивный журнал: Рекомендованный размер при еженедельном полном резервном копировании базы данных	132 ГБ [1]	Из-за требования возможности сохранения архивных журналов за три цикла резервного копирования базы данных сервера умножьте этот оценочный размер активного журнала на 3, чтобы оценить суммарные требования к размеру архивного журнала. Умножим этот результат на число дней между полными резервными копированиями базы данных:
		`(4 ГБ x 3 ) x 7 = 84 ГБ`
		Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
		`84 + 48 = 132 ГБ`

[1] Значения примера в этой таблице используются только, чтобы показать, как вычисляются размеры активных журналов и архивных журналов. В производственной среде, где не используется дедупликация, предлагаемый минимальный размер активного журнала - 16 ГБ. Рекомендуемый начальный размер архивного журнала в производственной среде, где не используется дедупликация, составляет 48 ГБ. Если при подстановке в приведенные оценки значений для вашей среды получатся результаты, превышающие 16 ГБ и 48 ГБ, используйте большие величины для оценки размера активного и архивного журнала.

Отслеживайте свои журналы и при необходимости настраивайте их размеры.

Пример: оценка размера активных и архивных журналов для операций дедупликации данных

Если используется дедупликация данных, необходимо рассмотреть ее влияние на требования к размеру пространства активных и архивных журналов.

Следующие факторы влияют на требования к размеру пространства активных и архивных журналов:

Объем дедуплицированных данных
Влияние дедупликации данных на размер активного и архивного журналов зависит от процентной доли данных, которые могут использоваться для дедупликации. Если эта процентная доля данных для дедупликации относительно велика, потребуется больший объем пространства журналов.

Размер и количество экстентов
Для каждого экстента, идентифицированного в процессе подготовки дедупликации, требуется примерно 1500 байт в пространстве активного журнала. Например, если при подготовке процесса дедупликации идентифицировано 250 тысяч экстентов, оценочный объем активного журнала составляет:

```
250 000 идентифицированных в каждом процессе экстентов x 1500 байт
 для каждого экстента = 358 МБ
```

Рассмотрим следующий сценарий: Триста клиентов архива резервных копий проводят каждую ночь до 100 тысяч операций резервного копирования файлов. Эти операции создают рабочую нагрузку в 30 миллионов файлов. Среднее количество экстентов для каждого файла - два. Следовательно, полное число экстентов - 60 миллионов, а для архивного журнала требуется 84 ГБ памяти:

```
60 000 000 экстентов x 1500 байт на каждый экстент = 84 ГБ
```

Процесс идентификации дубликатов оперирует с агрегатами файлов. Агрегат состоит из файлов, которые сохранены в данной транзакции, как задано опцией сервера TXNGROUPMAX. Предположим, что по умолчанию для опции сервера TXNGROUPMAX задано значение 4096. Если среднее число экстентов для каждого файла - два, общее число экстентов в каждом агрегате - 8192, а требуемая память активного журнала - 12 МБ:

```
8192 экстента в каждом агрегате x 1500 байт на каждый экстент =
   12 МБ
```

Время выполнения и число процессов идентификации дубликатов

Время выполнения и число процессов идентификации дубликатов также влияют на размер активного журнала. Если использовать оцененный в предыдущем примере размер активного журнала (12 МБ), при параллельном выполнении десяти процессов идентификации дубликатов одновременная нагрузка активного журнала составит 120 МБ:

```
12 МБ на каждый процесс x 10 процессов = 120 МБ
```

Размер файла

На размер активного журнала могут влиять также большие файлы, обрабатываемые для идентификации дубликатов. Допустим, например, что клиент резервного копирования и архивирования производит резервную копию около 80 гигабайтов (снимок файловой системы). В этом объекте может содержаться большое число дублированных экстентов, например, если проводилось инкрементное резервное копирование включенных в файловую систему файлов. Допустим, например, что снимок файловой системы содержит 1,2 миллиона дублированных экстентов. Эти 1,2 миллиона экстентов в таком большом файле представляют единственную транзакцию для процесса идентификации дубликатов. Требуемая для этого единственного объекта полная память активного журнала составляет 1,7 гигабайтов:

```
1 200 000 экстентов x 1500 байт на каждый экстент = 1,7 ГБ
```

Если одновременно с процессом идентификации дубликатов для этого большого объекта будет происходит аналогичный, но меньший по объему процесс, активному журналу может не хватить памяти. Допустим, например, что пул хранения включен для дедупликации. В пуле хранения содержится смесь данных, в том числе мелкие файлы с размером от 10 КБ до нескольких сотен КБ. В пуле хранения есть также несколько больших объектов, содержащих основную процентную долю дублированных экстентов.

Чтобы принять во внимание не только требования к объему памяти, но и затраты времени и продолжительность одновременных транзакций, увеличьте оцененный размер активного журнала примерно вдвое. Допустим, например, что ваша оценка дает для требуемого объема памяти значение 25 ГБ (23,3 ГБ + 1,7 ГБ на дедупликацию большого объекта). Если процессы дедупликации выполняются одновременно, рекомендуемый размер активного журнала составит 50 ГБ. Предлагаемый размер архивного журнала - 150 ГБ.

Примеры в следующих таблицах показывают результаты расчетов для активных и архивных журналов. В примере первой таблицы использован средний размер экстента 700 КБ. Во втором примере (вторая таблица) средний размер экстента - 256 КБ. Как видно, меньший средний размер дубликата экстента (256 КБ) приводит к большему оцененному размеру активного журнала. Для исключения или минимизации проблем функционирования сервера используйте значение 256 КБ для оценки размера активного журнала в вашей производственной среде.

Таблица 17. Средний размер дубликата экстента - 700 КБ

Элемент	Значения примера		Описание
Размер наибольшего единичного объекта для дедупликации	800 ГБ	4 ТБ	Детализация обработки для дедупликации - на уровне файлов. Поэтому наибольший единичный файл для дедупликации представляет собой наибольшую транзакцию и соответствующую большую нагрузку для активного и архивного журналов.

Таблица 17. Средний размер дубликата экстента - 700 КБ (продолжение)

Элемент	**Значения примера**		**Описание**
Средний размер экстентов	700 КБ	700 КБ	Алгоритмы дедупликации используют метод переменных блоков. Не у всех дедуплицированных экстентов данного файла одинаковый размер, поэтому для оценки используется средний размер экстентов.
Экстенты для данного файла	1 198 372 бит	6 135 667 бит	При использовании среднего размера экстентов (700 КБ) эта оценка дает среднее число экстентов для данного объекта. Для объекта размером 800 ГБ была использована следующая формула: `(800 ГБ ÷ 700 КБ) = 1 198 372 бит` Аналогичные вычисления для объекта размером 4 ТБ: `(4 ТБ ÷ 700 КБ) = 6 135 667`
Активный журнал: Оценочный размер, требуемый для дедупликации единичного большого объекта во время единичного процесса идентификации дубликатов	1,7 ГБ	8,6 ГБ	Оценка размера активного журнала, требуемого для этой транзакции.

Активный журнал: Рекомендуемый общий размер	66 ГБ [1]	79,8 ГБ [1]	Принимая во внимание другие аспекты рабочей нагрузки сервера в дополнение к дедупликации, увеличьте существующую оценку вдвое. В этих примерах требуемый для дедупликации единичного большого объекта размер памяти активного журнала рассматривается с учетом ранее полученной оценки требуемого размера активного журнала.
			В следующих вычислениях рассматривается несколько транзакций и объект размером 800 ГБ:
			`(23,3 ГБ + 1,7 ГБ) x 2 = 50 ГБ`
			Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
			`50 + 16 = 66 ГБ`
			В следующих вычислениях рассматривается несколько транзакций и объект размером 4 ТБ:
			`(23,3 ГБ + 8,6 ГБ) x 2 = 63,8 ГБ`
			Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
			`63,8 + 16 = 79,8 ГБ`

Таблица 17. Средний размер дубликата экстента - 700 КБ (продолжение)

Элемент	Значения примера		Описание

Архивный журнал: Рекомендуемый размер	198 ГБ [1]	239,4 ГБ [1]	Увеличьте оцененный размер активного журнала втрое.
			В следующих вычислениях рассматривается несколько транзакций и объект размером 800 ГБ:
			`50 ГБ x 3 = 150 ГБ`
			Увеличим этот размер на рекомендуемый начальный размер 48 ГБ:
			`150 + 48 = 198 ГБ`
			В следующих вычислениях рассматривается несколько транзакций и объект размером 4 ТБ:
			`63,8 ГБ x 3 = 191,4 ГБ`
			Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
			`191,4 + 48 = 239,4 ГБ`

[1] Значения примера в этой таблице используются только, чтобы показать, как вычисляются размеры активных журналов и архивных журналов. В производственной среде, где не используется дедупликация, рекомендуемый минимальный размер активного журнала - 32 ГБ. Рекомендуемый минимальный размер архивного журнала в производственной среде, где не используется дедупликация, составляет 96 ГБ. Если при подстановке в приведенные оценки значений для вашей среды получатся результаты, превышающие 32 ГБ и 96 ГБ, используйте большие величины для оценки размера активного и архивного журнала.

Отслеживайте свои журналы и при необходимости настраивайте их размеры.

Таблица 18. Средний размер дубликата экстента - 256 КБ

Элемент	Значения примера		Описание
Размер наибольшего единичного объекта для дедупликации	800 ГБ	4 ТБ	Детализация обработки для дедупликации - на уровне файлов. Поэтому наибольший единичный файл для дедупликации представляет собой наибольшую транзакцию и соответствующую большую нагрузку для активного и архивного журналов.
Средний размер экстентов	256 КБ	256 КБ	Алгоритмы дедупликации используют метод переменных блоков. Не у всех дедуплицированных экстентов данного файла одинаковый размер, поэтому для оценки используется средний размер экстентов.

Экстенты для данного файла	3 276 800 бит	16 777 216 бит	При использовании среднего размера экстентов эта оценка дает среднее число экстентов для данного объекта.
			В следующих вычислениях рассматривается несколько транзакций и объект размером 800 ГБ:
			`(800 ГБ ÷ 256 КБ) = 3 276 800 бит`
			В следующих вычислениях рассматривается несколько транзакций и объект размером 4 ТБ:
			`(4 ТБ ÷ 256 КБ) = 16 777 216 бит`

Таблица 18. Средний размер дубликата экстента - 256 КБ (продолжение)

Элемент	**Значения примера**		**Описание**
Активный журнал: Оценочный размер, требуемый для дедупликации единичного большого объекта во время единичного процесса идентификации дубликатов	4,5 ГБ	23,4 ГБ	Оценочный размер памяти активного журнала, требуемой для этой транзакции.

Активный журнал: Рекомендуемый общий размер	71,6 ГБ [1]	109,4 ГБ [1]	Принимая во внимание другие аспекты рабочей нагрузки сервера в дополнение к дедупликации, увеличьте существующую оценку вдвое. В этих примерах требуемый для дедупликации единичного большого объекта размер памяти активного журнала рассматривается с учетом ранее полученной оценки требуемого размера активного журнала.
			В следующих вычислениях рассматривается несколько транзакций и объект размером 800 ГБ:
			`(23,3 ГБ + 4,5 ГБ) x 2 = 55,6 ГБ`
			Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
			`55,6 + 16 = 71,6 ГБ`
			В следующих вычислениях рассматривается несколько транзакций и объект размером 4 ТБ:
			`(23,3 ГБ + 23,4 ГБ) x 2 = 93,4 ГБ`
			Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
			`93,4 + 16 = 109,4 ГБ`

Архивный журнал: Рекомендуемый размер	214,8 ГБ [1]	328,2 ГБ [1]	Троекратный размер оценки активного журнала.
			Следующие вычисления проведены для объекта размером 800 ГБ:
			`55,6 ГБ x 3 = 166,8 ГБ`
			Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
			`166,8 + 48 = 214,8 ГБ`
			Следующие вычисления проведены для объекта размером 4 ТБ:
			`93,4 ГБ x 3 = 280,2 ГБ`
			Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
			`280,2 + 48 = 328,2 ГБ`

Таблица 18. Средний размер дубликата экстента - 256 КБ (продолжение)

Элемент	Значения примера	Описание
[1] Значения примера в этой таблице используются только, чтобы показать, как вычисляются размеры активных журналов и архивных журналов. В производственной среде, где не используется дедупликация, рекомендуемый минимальный размер активного журнала - 32 ГБ. Рекомендуемый минимальный размер архивного журнала в производственной среде, где не используется дедупликация, составляет 96 ГБ. Если при подстановке в приведенные оценки значений для вашей среды получатся результаты, превышающие 32 ГБ и 96 ГБ, используйте большие величины для оценки размера активного и архивного журнала. Отслеживайте свои журналы и при необходимости настраивайте их размеры.		

Пространство зеркальной копии активного журнала

Можно использовать зеркальную копию активного журнала, если не удастся прочитать файлы активного журнала. Может существовать только одна зеркальная копия активного журнала.

Создание зеркальной копии журнала - рекомендуемая опция. Если вы увеличите размер активного журнала, размер зеркальной копии журнала увеличится автоматически. Зеркальное копирование журнала может отрицательно сказаться на производительности, так как при зеркальном копировании потребуется удвоенный объем операций ввода-вывода. Дополнительное пространство, которое требуется для зеркальной копии журнала - это еще один фактор, который следует учесть, при принятии решения относительно создания зеркальной копии журнала.

Если каталог зеркальной копии журнала переполняется, сервер записывает сообщения об ошибке в активный журнал и в файл `db2diag.log`. Работа сервера продолжится.

Пространство резервного архивного журнала

Резервный архивный журнал используется сервером, если в каталоге архивного журнала не хватает места.

Задав каталог резервного архивного журнала, можно предотвратить ошибки, которые могут происходить при нехватке места в каталоге архивного журнала. Если переполнятся и каталог архивного журнала, и диск или файловая система, где находится каталог резервного архивного журнала, данные останутся в каталоге активного журнала. Это условие может привести к остановке сервера в связи с переполнением активного журнала.

Мониторинг использования пространства для базы данных и журналов восстановления

Для определения размера используемого и доступного пространства активного журнала введите команду **QUERY LOG**. Для отслеживания использования пространства базой данных и журналами восстановления можно проверить также записи в журнале операций.

Активный журнал

Если объем доступного пространства активного журнала недостаточен, в журнале операций появятся следующие записи:

ANR4531I: IC_AUTOBACKUP_LOG_USED_SINCE_LAST_BACKUP_TRIGGER
Это сообщение выводится, когда объем пространства активного журнала превышает максимальный заданный размер. Сервер IBM Spectrum Protect начинает полное резервное копирование базы данных.

Чтобы изменить максимальный размер журнала, остановите сервер. Откройте файл `dsmserv.opt` и задайте новое значение для опции `ACTIVELOGSIZE`. По завершении операции перезапустите сервер.

ANR0297I: IC_BACKUP_NEEDED_LOG_USED_SINCE_LAST_BACKUP
Это сообщение выводится, когда объем пространства активного журнала превышает максимальный заданный размер. Надо вручную выполнить резервное копирование базы данных.

Чтобы изменить максимальный размер журнала, остановите сервер. Откройте файл `dsmserv.opt` и задайте новое значение для опции `ACTIVELOGSIZE`. По завершении операции перезапустите сервер.

ANR4529I: IC_AUTOBACKUP_LOG_UTILIZATION_TRIGGER
Отношение размера используемого пространства активного журнала к доступному размеру пространства активного журнала превышает порог использования журнала. Если должно будет начаться хотя бы одно полное резервное копирование базы данных, сервер IBM Spectrum Protect начнет инкрементное резервное копирование базы данных. В противном случае сервер начнет полное резервное копирование базы данных.

ANR0295I: IC_BACKUP_NEEDED_LOG_UTILIZATION
Отношение размера используемого пространства активного журнала к доступному размеру пространства активного журнала превышает порог использования журнала. Надо вручную выполнить резервное копирование базы данных.

Архивный журнал

Если объем доступного пространства архивного журнала недостаточен, в журнале операций появится следующая запись:

ANR0299I: IC_BACKUP_NEEDED_ARCHLOG_USED
Отношение размера используемого пространства архивного журнала к доступному размеру пространства архивного журнала превышает порог использования журнала. Сервер IBM Spectrum Protect начинает автоматическое полное резервное копирование базы данных.

База данных

Если объем доступного пространства для операций базы данных недостаточен, в журнале операций появятся следующие сообщения:

ANR2992W: IC_LOG_FILE_SYSTEM_UTILIZATION_WARNING_2
Используемое пространство базы данных превышает порог использования пространства базы данных. Чтобы увеличить размер пространства для базы данных, используйте команду **EXTEND DBSPACE**, команду **EXTEND DBSPACE** или утилиту DSMSERV FORMAT с параметром **DBDIR**.

ANR1546W: FILESYSTEM_DBPATH_LESS_1GB
Размер доступного пространства в каталоге, где расположены серверные файлы базы данных, меньше 1 ГБ.

Когда сервер IBM Spectrum Protect создается при помощи утилиты DSMSERV FORMAT или мастера по конфигурированию, одновременно создаются база данных сервера и журнал восстановления. Кроме того, создаются файлы для хранения информации о базе данных, используемой менеджером базы данных. Указанный в этом сообщении каталог обозначает положение информации о базе данных, используемой менеджером баз данных. Если в этом каталоге нет доступного пространства, сервер больше не может функционировать.

Необходимо добавить пространство к файловой системе или обеспечить доступное пространство в файловой системе или на диске.

Удаление файлов отката установки

Можно удалить определенные файлы установки, сохраненные во время процесса установки, чтобы высвободить пространство в каталоге совместно используемого ресурса. Например, файлы, которые, возможно, требовались для операции отката, это те файлы, которые можно удалить.

Об этой задаче

Чтобы удалить файлы, которые больше не нужны, используйте либо графический мастер установки, либо командную строку в режиме консоли.

Удаление файлов отката установки с использованием графического мастера

Можно удалить определенные файлы установки, сохраненные во время процесса установки, используя пользовательский интерфейс IBM Installation Manager.

Процедура

1. Откройте IBM Installation Manager.

   В каталоге, в котором установлен IBM Installation Manager, перейдите в подкаталог `eclipse` (например, `/opt/IBM/InstallationManager/eclipse`) и введите следующую команду, чтобы запустить IBM Installation Manager:

   ```
   ./IBMIM
   ```

2. Щелкните по **Файл** > **Предпочтения**.
3. Выберите **Файлы для отката**.
4. Щелкните по **Удалить сохраненные файлы** и нажмите кнопку **OK**.

Удаление файлов отката установки с использованием командной строки

Можно удалить определенные файлы установки, сохраненные во время процесса установки, при помощи командной строки.

Процедура

1. В каталоге, в котором установлен IBM Installation Manager, перейдите в следующий подкаталог:

   ```
   eclipse/tools
   ```

   Например:

   ```
   /opt/IBM/InstallationManager/eclipse/tools
   ```

2. В каталоге `tools` введите следующую команду, чтобы запустить командную строку IBM Installation Manager:

   ```
   ./imcl -c
   ```

3. Введите П, чтобы выбрать **Предпочтения**.
4. Введите 3, чтобы выбрать **Файлы для отката**.
5. Введите D, чтобы **удалить файлы для отката**.
6. Введите A, чтобы **применить изменения и вернуться в меню предпочтений**.
7. Введите C, чтобы выйти из **Меню предпочтений**.
8. Введите X, чтобы **закрыть Installation Manager**.

Практические рекомендации по именованию сервера

Используйте эти описания для справки при установке или обновлении сервера IBM Spectrum Protect.

ID пользователя экземпляра

ID пользователя экземпляра служит основой для других имен, связанных с экземпляром сервера. ID пользователя экземпляра также называют владельцем экземпляра.

Например: tsminst1

ID пользователя экземпляра - это ID пользователя, у которого должны быть полномочия владельца или доступ с правом на чтение/запись для всех каталогов, которые вы создаете для базы данных и журнала восстановления. Обычная практика работы сервера - его запуск от имени ID пользователя экземпляра. У этого ID пользователя должно быть право чтения и записи в каталоги, используемые для всех классов устройств **FILE**.

Домашний каталог для ID пользователя экземпляра

Домашний каталог (если он еще не существует) можно создать при создании ID пользователя экземпляра, указав для этого опцию `-m`. В зависимости от локальных параметров имя домашнего каталога может иметь следующий вид: `/home/`*`ID_пользователя_экземпляра`*.

Например: `/home/tsminst1`

Домашний каталог изначально используется для содержания профиля ID пользователя и параметров безопасности.

Имя экземпляра базы данных

Имя экземпляра базы данных должно совпадать с ID пользователя экземпляра, от имени которого вы запускаете экземпляр сервера.

Например: `tsminst1`

Каталог экземпляра

Каталог экземпляра - это каталог, содержащий связанные с экземпляром сервера файлы (файл опций сервера и другие специфичные для сервера файлы). У этого каталога может быть любое имя по вашему выбору. Чтобы этот каталог было проще распознать, используйте имя, связывающее каталог с именем экземпляра.

Каталог экземпляра можно создать как подкаталог домашнего каталога ID пользователя экземпляра. Например: `/home/`*`ID_пользователя_экземпляра`*`/`*`ID_пользователя_экземпляра`*

В приведенном ниже примере каталог экземпляра размещается в домашнем каталоге для пользователя с ID tsminst1: `/home/tsminst1/tsminst1`

Этот каталог также можно создать в другом месте, например: `/tsmserver/tsminst1`

В каталоге экземпляра хранятся следующие файлы для экземпляра сервера:

- Файл серверных опций, `dsmserv.opt`
- Файл базы данных ключей сервера `cert.kdb` и файлы `.arm` (используемые клиентами и другими серверами для импорта сертификатов **SSL** на сервер)
- Файл конфигурации устройств, если серверная опция `DEVCONFIG` не задает полное имя
- Файл истории томов, если серверная опция `VOLUMEHISTORY` не задает полное имя
- Тома для пулов хранения **DEVTYPE**=**FILE**, если спецификация каталога для класса устройств не является полной.
- Обработчики пользователя
- Выходная информация трассировки (если не задано полное имя)

Имя базы данных

Именем базы данных для каждого экземпляра сервера всегда является TSMDB1. Это имя нельзя изменить.

Имя сервера

Имя сервера - это внутреннее имя для IBM Spectrum Protect, и оно используется для выполнения операций, включающих в себя взаимодействия между несколькими серверами IBM Spectrum

Protect. В качестве примера можно привести взаимодействие сервера с сервером и совместное использование библиотеки.

Имя сервера также используется при добавлении сервера в Центр операций, чтобы им можно было управлять с использованием этого интерфейса. Используйте для каждого сервера уникальное имя. Чтобы имя было проще распознать в интерфейсе Центра операций (или в выходной информации команды **QUERY SERVER**), используйте имя, отражающее расположение или назначение сервера. Не изменяйте имя сервера IBM Spectrum Protect после того, как он сконфигурирован как хаб или подчиненный сервер.

Если вы используете мастер, рекомендуемым именем по умолчанию будет имя хоста компьютера, который вы используете. Можно использовать другое имя, которое будет иметь смысл в вашей среде. Если у вас в системе более одного сервера и вы используете мастер, вы сможете использовать имя по умолчанию только для одного из серверов. Для каждого сервера нужно ввести уникальное имя.

Например:

```
PAYROLL
SALES
```

Каталоги для пространства базы данных и журнала восстановления

Каталогам можно присваивать имена в соответствии с принятой у вас практикой. Чтобы было проще распознавать каталоги, используйте имена, связывающие каталоги с экземпляром сервера.

Например, в случае архивного журнала:

```
/tsminst1_archlog
```

Каталоги установки

К каталогам установки сервера IBM Spectrum Protect относятся каталог сервера, каталог IBM Db2, каталог устройств, каталог языка и другие каталоги. В каждом из них содержится несколько дополнительных каталогов.

(`/opt/tivoli/tsm/server/bin`) - это каталог по умолчанию, содержащий код сервера и файлы лицензии.

Структура каталогов продукта Db2, устанавливаемого в ходе установки сервера IBM Spectrum Protect, соответствует тому, что задокументировано в источниках информации по Db2. Защищайте эти каталоги и файлы так же, как вы защищаете каталоги сервера. Каталог по умолчанию - `/opt/tivoli/tsm/db2`.

Можно использовать следующий языки: английский (США), испанский, итальянский, китайский Big5, китайский GBK, китайский традиционный, китайский упрощенный, корейский, немецкий, португальский (Бразилия), русский, французский и японский.

Глава 2. Установка компонентов сервера

Чтобы установить компоненты сервера IBM Spectrum Protect, можно использовать либо мастер установки, либо командную строку в режиме консоли.

Об этой задаче

При использовании программы установки IBM Spectrum Protect можно установить следующие компоненты:

- сервер

  Совет: База данных (IBM Db2), Global Security Kit (GSKit) и IBM Java Runtime Environment (JRE) автоматически устанавливаются при выборе компонента сервера.
- языки сервера
- лицензия
- устройства
- IBM Spectrum Protect for SAN
- Центр операций

Отведите для установки сервера в соответствии с данным руководством примерно 30-45 минут.

Получение пакета установки

Пакет установки IBM Spectrum Protect можно получить с сайта скачивания IBM (например, Passport Advantage или IBM Fix Central).

Прежде чем начать

Если вы собираетесь скачать эти файлы, задайте неограниченный системный предел пользователя для максимального размера файла, чтобы файлы были успешно скачаны:

1. Чтобы запросить значение для максимального размера файла, введите следующую команду:

   ```
   ulimit -Hf
   ```
2. Если системный пользовательский предел на максимальный размер файла не задан неограниченным, измените его на неограниченный, следуя инструкциям в документации для вашей операционной системы.

Процедура

1. Загрузите нужный файл пакета с одного из следующих веб-сайтов.
   - Скачайте пакет сервера со страницы Passport Advantage или Fix Central.
   - Самую свежую информацию, обновления и исправления обслуживания смотрите по адресу: IBM Support Portal.
2. Если вы скачали пакет с сайта скачивания IBM, то сделайте следующее:
   a. Убедитесь, что у вас будет достаточно места для хранения файлов установки, когда они будут извлечены из пакета продукта. Требования к свободному месту можно увидеть в документе по скачиванию:
      - IBM Spectrum Protect technote 588021
      - IBM Spectrum Protect Extended Edition technote 588023
      - IBM Spectrum Protect for Data Retention technote 588025

b. Скачайте файл пакета в каталог по вашему выбору. Имя каталога может содержать не более 128 символов. Убедитесь, что извлекаете файлы установки в пустой каталог. Не выполняйте извлечение в каталог с ранее извлеченными файлами или с какими-либо еще файлами.

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

```
chmod a+x имя_пакета.bin
```

d. Извлеките пакет, введя следующую команду:

```
./имя_пакета.bin
```

где *имя_пакета* - это имя скачанного файла, например:

```
8.1.x.000-IBM-SPSRV-Linuxx86_64.bin
8.1.x.000-IBM-SPSRV-Linuxs390x.bin
8.1.x.000-IBM-SPSRV-Linuxppc64le.bin
```

3. Выберите один из следующих способов установки IBM Spectrum Protect:
   - “Установка IBM Spectrum Protect при помощи мастера установки” на стр. 86
   - “Установка IBM Spectrum Protect в режиме консоли” на стр. 87
   - “Установка IBM Spectrum Protect в режиме без вывода сообщений” на стр. 87
4. После установки IBM Spectrum Protect и до настройки этого продукта в соответствии с вашими требованиями посетите следующий веб-сайт:

   IBM Support Portal. Щелкните по **Support and downloads** (Поддержка и материалы для скачивания) и примените все требуемые исправления.

Установка IBM Spectrum Protect при помощи мастера установки

Сервер можно установить при помощи графического мастера IBM Installation Manager.

Прежде чем начать

Перед запуском установки сделайте следующее:

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

Процедура

Установите IBM Spectrum Protect, используя следующий метод:

Опция	Описание
Установка программы из скачанного пакета:	a. Перейдите в каталог, в который вы скачали пакет.. b. Запустите мастер установки, введя следующую команду: `./install.sh`

Дальнейшие действия

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

  Вы можете просмотреть файлы журнала установки, выбрав **Файл** > **Просмотреть журнал** в инструменте Installation Manager. Чтобы выполнить сбор этих файлов журнала, выберите **Справка** > **Экспорт данных для анализа проблем** в инструменте Installation Manager.

- После установки сервера и компонентов и до настройки этого продукта в соответствии с вашими требованиями посетите сайт IBM Support Portal. Щелкните по **Downloads (fixes and PTFs)** (Скачивание: исправления и PTF) и примените все требуемые исправления.
- После установки нового сервера ознакомьтесь с разделом Глава 3, “Первые шаги после установки IBM Spectrum Protect”, на стр. 91, чтобы узнать, как сконфигурировать сервер.

Установка IBM Spectrum Protect в режиме консоли

IBM Spectrum Protect можно установить из командной строки в режиме консоли.

Прежде чем начать

Перед запуском установки сделайте следующее:

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

Процедура

Установите IBM Spectrum Protect, используя следующий метод:

Опция	Описание
Установка программы из скачанного пакета:	a. Перейдите в каталог, в который вы скачали пакет.. b. Запустите мастер установки в консольном режиме, введя следующую команду: `./install.sh -c` **Необязательно:** Сгенерируйте файл ответов в ходе установки в режиме консоли. Укажите опции установки в режиме консоли и на панели **Сводка** укажите G, чтобы сгенерировать ответы.

Дальнейшие действия

- Если в процессе установки возникают ошибки, то они записываются в файлы журнала, которые хранятся в каталоге журналов IBM Installation Manager, например:

  `/var/ibm/InstallationManager/logs`
- После установки сервера и компонентов и до настройки этого продукта в соответствии с вашими требованиями посетите сайт IBM Support Portal. Щелкните по **Downloads (fixes and PTFs)** (Скачивание: исправления и PTF) и примените все требуемые исправления.
- После установки нового сервера ознакомьтесь с разделом Глава 3, “Первые шаги после установки IBM Spectrum Protect”, на стр. 91, чтобы узнать, как сконфигурировать сервер.

Установка IBM Spectrum Protect в режиме без вывода сообщений

Сервер можно установить или обновить в режиме без вывода сообщений. В режиме без вывода сообщений установка не отправляет сообщений на консоль, а сохраняет сообщения и ошибки в файлы журнала.

Прежде чем начать

Чтобы задать входные данные при использовании установки в режиме без вывода сообщений, можно использовать файл ответов. Указанные ниже примеры файлов ответов поставляются в каталоге `input` в том месте, куда был распакован пакет установки:

`install_response_sample.xml`
Используйте этот файл для установки компонентов IBM Spectrum Protect.

`update_response_sample.xml`
Используйте этот файл для обновления компонентов IBM Spectrum Protect.

Эти файлы содержат значения по умолчанию, которые помогут вам избежать всех ненужных предупреждений. Чтобы воспользоваться этими файлами, выполните приведенные в файлах инструкции.

Если вы хотите настроить файл ответов, вы можете изменить опции, содержащиеся в файле. Информацию о файлах ответов смотрите в разделе Файлы ответов.

Процедура

1. Создайте файл ответов.

   Вы можете изменить пример файла ответов или создать свой собственный.
2. Если вы устанавливаете сервер и компонент Центр операций в режиме без вывода сообщений, создайте пароль для склада доверенных сертификатов компонента Центр операций в файле ответов.

   Если вы используете файл `install_response_sample.xml`, добавьте пароль в следующую строку в файле, где *пароль* - это пароль:

   ```
   <variable
   name='ssl.password' value='пароль' />
   ```

   Дополнительную информацию об этом пароле смотрите в разделе Контрольный список установки.

   Совет: Пароль склада доверенных сертификатов не требуется, если вы используете файл `update_response_sample.xml` для обновления компонента Центр операций.
3. Запустите установку без вывода сообщений, введя в каталоге, в который распакован пакет установки, следующую команду. Значение *файл_ответов* соответствует пути и имени файла ответов:

   - ```
     ./install.sh -s -input файл_ответов
     -acceptLicense
     ```

Дальнейшие действия

- Если в процессе установки возникают ошибки, то они записываются в файлы журнала, которые хранятся в каталоге журналов IBM Installation Manager, например:

  ```
  /var/ibm/InstallationManager/logs
  ```
- После установки сервера и компонентов и до настройки этого продукта в соответствии с вашими требованиями посетите сайт IBM Support Portal. Щелкните по **Downloads (fixes and PTFs)** (Скачивание: исправления и PTF) и примените все требуемые исправления.
- После установки нового сервера ознакомьтесь с разделом Глава 3, “Первые шаги после установки IBM Spectrum Protect”, на стр. 91, чтобы узнать, как сконфигурировать сервер.
  ```

Установка языковых пакетов сервера

Переводы для сервера позволяют серверу показывать сообщения и справку на языках, отличных от английского (США). Такие переводы позволяют также использовать региональные стандарты представления дат, времени и чисел.

Прежде чем начать

Инструкции по установке пакетов поддержки национальных языков для агента хранения смотрите в документе Конфигурация пакета поддержки национальных языков для агентов хранения.

Локали языка сервера

Либо используйте опцию языкового пакета по умолчанию, либо выберите другой языковой пакет для вывода сообщений и справки сервера.

Этот языковый пакет автоматически устанавливается для следующей языковой опции по умолчанию для сообщений и справки сервера IBM Spectrum Protect:

- LANGUAGE en_US

Для прочих языков и локалей установите языковой пакет, нужный для вашей установки.

Можно использовать следующие языки:

Таблица 19. Языки сервера для Linux

LANGUAGE	**Значение опции LANGUAGE**
Китайский упрощенный	zh_CN
	zh_CN.gb18030
	zh_CN.utf8
Китайский традиционный	Big5 / Zh_TW
	zh_TW
	zh_TW.utf8
Английский, США	en_US
	en_US.utf8
Французский	fr_FR
	fr_FR.utf8
Немецкий	de_DE
	de_DE.utf8
Итальянский	it_IT
	it_IT.utf8
Японский	ja_JP
	ja_JP.utf8
Корейский	ko_KR
	ko_KR.utf8
Бразильский португальский	pt_BR
	pt_BR.utf8

Таблица 19. Языки сервера для Linux (продолжение)	
LANGUAGE	**Значение опции LANGUAGE**
Русский	ru_RU
	ru_RU.utf8
Испанский	es_ES
	es_ES.utf8

Ограничение: При использовании Центра операций некоторые символы могут выводиться неправильно, если язык веб-браузера не совпадает с языком сервера. При появлении этой неполадки следует сконфигурировать в браузере использование того же языка, что и на сервере.

Конфигурирование языкового пакета

После конфигурирования языкового пакета сообщения и справки выводятся на сервере на языке, отличном от английского (США). Пакеты установки входят в комплект поставки программного обеспечения IBM Spectrum Protect.

Об этой задаче

Для задания поддержки определенной локали выполните одну из следующих задач:

- Для опции LANGUAGE в файле опций сервера задайте имя локали, которую нужно использовать. Например:

  Чтобы использовать локаль `ru_RU.UTF-8`, задайте для опции LANGUAGE значение `ru_RU.UTF-8`. Смотрите раздел “Локали языка сервера” на стр. 89.
- Если вы запускаете сервер в режиме активного окна, то задайте для переменной среды LC_ALL значение, совпадающее со значением, которое задано в файле опций сервера. Например, чтобы задать переменную среды для русского языка, введите следующее значение:

```
export LC_ALL=ru_RU.UTF-8
```

Если локаль успешно инициализирована, то с ее помощью форматируется дата, время и представление чисел для сервера. Если локаль не инициализируется успешно, сервер будет использовать файлы сообщений на английском языке (США), а также формат дат времени и чисел для языка системы 'Английский (США)'.

Обновление языкового пакета

Вы можете изменить или обновить языковой пакет при помощи IBM Installation Manager.

Об этой задаче

Внутри одного и того же экземпляра IBM Spectrum Protect можно установить другой языковой пакет.

- Для установки другого языкового пакета используйте функцию **Изменить** программы IBM Installation Manager.
- Для обновления языковых пакетов до новых версий используйте функцию **Обновить** программы IBM Installation Manager.

Совет: В IBM Installation Manager термин *обновить* (update) означает поиск и установку обновлений и исправлений для установленных программных пакетов. В этом контексте термины *update* и *upgrade* являются синонимами.

Глава 3. Первые шаги после установки IBM Spectrum Protect

После установки компонента IBM Spectrum Protect подготовьтесь к конфигурированию. Использование мастера по конфигурированию - предпочтительный способ для конфигурирования экземпляра IBM Spectrum Protect.

Об этой задаче

1. Измените значения параметров ядра. Смотрите раздел Настройка параметров ядра для систем Linux.
2. Создайте каталоги и ID пользователя для экземпляра сервера. Смотрите раздел “Создание ID пользователя и каталогов для экземпляра сервера” на стр. 93.
3. Сконфигурируйте экземпляр сервера. Выберите одну из следующих опций.
   - Воспользуйтесь мастером по конфигурированию - это рекомендуемый способ. Смотрите раздел “Конфигурирование IBM Spectrum Protect при помощи мастера конфигурирования” на стр. 95.
   - Сконфигурируйте вручную новый экземпляр. Смотрите раздел “Конфигурирование экземпляра сервера вручную” на стр. 95. При конфигурировании вручную выполните описанные ниже шаги.
     a. Сконфигурируйте каталоги и создайте экземпляр IBM Spectrum Protect. Смотрите раздел “Создание экземпляра сервера” на стр. 96.
     b. Создайте новый файл серверных опций, скопировав пример файла, чтобы сконфигурировать связь между сервером и клиентами. Смотрите раздел “Конфигурирование связи между сервером и клиентом” на стр. 97.
     c. Введите команду **DSMSERV FORMAT**, чтобы сформатировать базу данных. Смотрите раздел “Форматирование базы данных и журнала” на стр. 100.
     d. Сконфигурируйте систему для резервного копирования базы данных. Смотрите раздел “Подготовка менеджера базы данных к резервному копированию базы данных” на стр. 101.
4. Сконфигурируйте опции, чтобы управлять временем запуска реорганизации базы данных. Смотрите раздел “Опции конфигурирования сервера для обслуживания сервера баз данных” на стр. 104.
5. Запустите экземпляр сервера, если он еще не запущен.

   Смотрите раздел “Запуск экземпляра сервера” на стр. 105.
6. Зарегистрируйте свою лицензию. Смотрите раздел “Регистрация лицензий” на стр. 111.
7. Подготовьте систему для резервного копирования базы данных. Смотрите раздел “Подготовка сервера к операциям резервного копирования базы данных ” на стр. 111.
8. Чтобы упростить устранение неполадок на случай возникновения в будущем каких-либо проблем, убедитесь, что для дампа ядра выделено достаточно пространства. Дополнительную информацию смотрите в техническом замечании 6357399.
9. Производите мониторинг сервера. Смотрите раздел “Мониторинг сервера” на стр. 112.

Настройка параметров ядра

Для правильной установки и работы IBM Spectrum Protect и IBM Db2 в Linux надо изменить параметры конфигурации ядра.

Об этой задаче

Если вы не измените эти параметры, установка Db2 и IBM Spectrum Protect может завершиться неудачно. И даже при успешной установке при работе могут возникнуть проблемы.

Изменение параметров ядра

IBM Db2 автоматически увеличивает значения параметров ядра межпроцессовой связи (interprocess communication, IPC) до предпочтительных.

Об этой задаче

Чтобы изменить параметры ядра на сервере Linux, выполните следующие действия:

Процедура

1. Введите команду **ipcs -l**, чтобы вывести список значений параметров.
2. Проанализируйте результаты, чтобы определить, требуются ли какие-либо изменения для вашей системы.

   Если требуются изменения, можно задать параметр в файле `/etc/sysctl.conf`. Это значение параметра применяется при запуске системы.

Дальнейшие действия

Для Red Hat Enterprise Linux 6 (RHEL6) надо задать параметр `kernel.shmmax` в файле `/etc/sysctl.conf` до автоматического перезапуска сервера IBM Spectrum Protect при запуске системы.

Подробную информацию о базе данных Db2 для Linux смотрите по адресу: Информация о продукте Db2.

Рекомендуемые значения

Убедитесь, что значения параметров ядра достаточны для исключения проблем при работе сервера IBM Spectrum Protect.

Об этой задаче

В следующей таблице содержатся описания параметров ядра для работы как IBM Spectrum Protect, так и IBM Db2.

Оптимальные значения параметров ядра	
Параметр	**Описание**
kernel.randomize_va_space	Параметр **kernel.randomize_va_space** конфигурирует использование памяти ASLR для ядра. Отключите ASLR, так как это может вызвать ошибки в программе Db2. Дополнительные подробности об ASLR Linux и Db2 смотрите в техническом замечании по адресу: http://www.ibm.com/support/docview.wss?uid=swg21365583.
vm.swappiness	Параметр **vm.swappiness** определяет, может ли ядро выполнять своппинг для памяти программы из физической оперативной памяти. Дополнительную информацию о параметрах ядра смотрите по адресу Информация о продукте Db2.

Оптимальные значения параметров ядра *(продолжение)*	
Параметр	**Описание**
vm.overcommit_memory	Параметр **vm.overcommit_memory** влияет на то, какой объем виртуальной памяти ядро позволяет размещать. Дополнительную информацию о параметрах ядра смотрите по адресу Информация о продукте Db2.

Создание ID пользователя и каталогов для экземпляра сервера

Создайте ID пользователя для экземпляра сервера IBM Spectrum Protect и каталоги, которые нужны экземпляру сервера для базы данных и журналов восстановления.

Прежде чем начать

Прежде чем выполнять данную задачу, ознакомьтесь с информацией о планировании пространства для сервера. Смотрите раздел “Контрольные списки для планирования сведений о сервере” на стр. 61.

Процедура

1. Создайте ID пользователя, который станет владельцем экземпляра сервера.

   Вы будете использовать этот ID пользователя при создании экземпляра сервера в одном из последующих шагов.

   Создайте ID пользователя и группу, которые станут владельцем экземпляра сервера.

   a. От имени ID пользователя - администратора можно запустить следующие команды конфигурирования пользователей и групп. Создайте ID пользователя и группу в домашнем каталоге пользователя.

      Ограничение: В ID пользователя можно использовать буквы нижнего регистра (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.

      Например, создайте ID пользователя `tsminst1` в группе `tsmsrvrs`. В приведенных ниже примерах показано, как создать этот ID пользователя и эту группу при помощи команд операционной системы.

      ```
      groupadd tsmsrvrs -g 1111
      useradd -d /home/tsminst1 -u 2222 -g 1111 -s /bin/bash tsminst1
      passwd tsminst1
      ```

      Ограничение: IBM Db2 не поддерживает непосредственную аутентификацию пользователя системы через LDAP.

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

2. Создайте каталоги, необходимые серверу.

Создайте пустые каталоги для каждого элемента в таблице и убедитесь, что каталогами владеет новый ID пользователя, который вы только что создали. Смонтируйте связанную систему хранения каждому каталогу для активного и архивного журнала, а также для каталогов базы данных.		
Элемент	**Примеры команд для создания каталогов**	**Ваши каталоги**
Каталог экземпляра для сервера, представляющий собой каталог с файлами, связанными именно с данным экземпляром сервера (файл серверных опций и другие файлы, связанные с сервером)	`mkdir /tsminst1`	

Каталоги базы данных	`mkdir /tsmdb001`
	`mkdir /tsmdb002`
	`mkdir /tsmdb003`
	`mkdir /tsmdb004`	

Каталог активного журнала	`mkdir /tsmlog`	
Каталог архивного журнала	`mkdir /tsmarchlog`	
Необязательно: Каталог для зеркальной копии активного журнала	`mkdir /tsmlogmirror`	
Необязательно: Каталог вторичного архивного журнала (каталог для резервного архивного журнала)	`mkdir /tsmarchlogfailover`	

При первоначальном создании сервера при помощи утилиты **DSMSERV FORMAT** или мастера конфигурирования создается база данных сервера и журнал восстановления. Кроме того, создаются файлы для хранения информации о базе данных, используемой менеджером базы данных.

3. Завершите сеанс для нового ID пользователя.

Конфигурирование сервера IBM Spectrum Protect

После того как вы установите сервер и подготовитесь к конфигурированию, сконфигурируйте экземпляр сервера.

Об этой задаче

Сконфигурируйте экземпляр сервера IBM Spectrum Protect, выбрав один из следующих вариантов:

- Воспользуйтесь мастером конфигурирования IBM Spectrum Protect на локальном компьютере. Смотрите раздел “Конфигурирование IBM Spectrum Protect при помощи мастера конфигурирования” на стр. 95.

- Сконфигурируйте вручную новый экземпляр IBM Spectrum Protect. Смотрите раздел “Конфигурирование экземпляра сервера вручную” на стр. 95. При конфигурировании вручную выполните описанные ниже шаги.

  1. Сконфигурируйте каталоги и создайте экземпляр IBM Spectrum Protect. Смотрите раздел “Создание экземпляра сервера” на стр. 96.
  2. Создайте новый файл серверных опций, скопировав пример файла, чтобы сконфигурировать связь между сервером и клиентами IBM Spectrum Protect. Смотрите раздел “Конфигурирование связи между сервером и клиентом” на стр. 97 .
  3. Введите команду DSMSERV FORMAT, чтобы сформатировать базу данных. Смотрите раздел “Форматирование базы данных и журнала” на стр. 100.
  4. Сконфигурируйте систему для резервного копирования базы данных. Смотрите раздел “Подготовка менеджера базы данных к резервному копированию базы данных” на стр. 101.

Конфигурирование IBM Spectrum Protect при помощи мастера конфигурирования

Мастер обеспечивает подход к конфигурированию сервера на основе набора шагов. Используя графический интерфейс пользователя, вы сможете обойти ряд шагов по конфигурированию, которые сложно выполнить вручную. Запустите мастер в системе, в которой вы установили программу сервера IBM Spectrum Protect.

Прежде чем начать

Прежде чем использовать мастер конфигурирования, нужно выполнить все предыдущие шаги для подготовки к конфигурированию. В число этих шагов входят установка IBM Spectrum Protect, создание каталогов базы данных и журналов и создание каталогов и ID пользователя для экземпляра сервера.

Процедура

1. Убедитесь, что выполнены следующие требования:
   - 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 систему, 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.
2. Запустите локальную версию мастера:

   Откройте программу `dsmicfgx` в каталоге `/opt/tivoli/tsm/server/bin`. Этот мастер можно запускать только с использованием ID пользователя root.

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

Конфигурирование экземпляра сервера вручную

После установки IBM Spectrum Protect вы можете сконфигурировать IBM Spectrum Protect вручную, а не при помощи мастера конфигурирования.

Создание экземпляра сервера

Создайте экземпляр IBM Spectrum Protect, введя команду **db2icrt**.

Об этой задаче

На одной рабочей станции может быть один или несколько экземпляров сервера.

Важное замечание: Прежде чем вводить команду **db2icrt**, убедитесь в следующем:

- Существует домашний каталог для пользователя (/home/tsminst1). Если домашнего каталога нет, вы должны его создать.

  В каталоге экземпляра хранятся следующие файлы, сгенерированные сервером IBM Spectrum Protect:

  – Файл серверных опций, dsmserv.opt
  – Файл базы данных ключей сервера cert.kdb и файлы .arm (используемые клиентами и другими серверами для импорта сертификатов **SSL** на сервер)
  – Файл конфигурации устройств, если серверная опция DEVCONFIG не задает полное имя
  – Файл истории томов, если серверная опция VOLUMEHISTORY не задает полное имя
  – Тома для пулов хранения **DEVTYPE**=**FILE**, если спецификация каталога для класса устройств не является полной.
  – Обработчики пользователя
  – Выходная информация трассировки (если не задано полное имя)
- Резервную копию следующих файлов нужно сохранить в безопасном и защищенном месте:
  – Файлы главного ключа шифрования (dsmkeydb.*)
  – Сертификат сервера и файлы секретных ключей (cert.*)
- У пользователя root и ID пользователя экземпляра должны быть разрешения на запись в файл конфигурации оболочки. В домашнем каталоге существует файл конфигурации оболочки (например, .profile). Дополнительную информацию смотрите на веб-сайте Информация о продукте Db2. Найдите информацию о переменных среды Linux и UNIX.

1. Войдите в систему с ID пользователя root и создайте экземпляр IBM Spectrum Protect. Имя экземпляра должно совпадать с именем пользователя, являющегося владельцем экземпляра. Введите команду **db2icrt** в виде одной строки:

   ```
   /opt/tivoli/tsm/db2/instance/db2icrt -a server -u
   имя_экземпляра имя_экземпляра
   ```

   Например, если ID пользователя данного экземпляра - tsminst1, создайте экземпляр, введя следующую команду: Введите команду в одной строке.

   ```
   /opt/tivoli/tsm/db2/instance/db2icrt -a server -u
   tsminst1 tsminst1
   ```

   Напоминание: С этого момента используйте этот новый ID пользователя при конфигурировании сервера IBM Spectrum Protect. Завершите сеанс ID пользователя root и войдите в систему от имени нового ID пользователя-владельца экземпляра.
2. Измените каталог по умолчанию для базы данных, так чтобы он совпадал с каталогом экземпляра сервера. Если у вас несколько серверов, войдите в систему от имени ID пользователя экземпляра для каждого сервера. Введите команду:

   ```
   db2 update dbm cfg using dftdbpath каталог_экземпляра
   ```

   Например, если значением каталог_экземпляра является ID пользователя экземпляра:

   ```
   db2 update dbm cfg using dftdbpath /tsminst1
   ```
3. Измените путь библиотеки, включив в него библиотеки, необходимые для операций сервера.

Совет: В следующих примерах используются следующие каталоги:

- *каталог_bin_сервера* - это подкаталог каталога установки сервера. Например, /opt/tivoli/tsm/server/bin.
- *домашний_каталог_пользователей_экземпляра* - это домашний каталог пользователя экземпляра. Например, /home/tsminst1.

.

- Надо изменить один из следующих файлов, чтобы задать путь библиотек, когда запускаются IBM Db2 или сервер. Произведите обновление для оболочки, для использования которой сконфигурирован экземпляр пользователя.

  Оболочка Bash или Korn:

  ```
  домашний_каталог_пользователей_экземпляра/sqllib/userprofile
  ```

  Оболочка C:

  ```
  домашний_каталог_пользователей_экземпляра/sqllib/usercshrc
  ```

- Произведите обновление для оболочки, для использования которой сконфигурирован экземпляр пользователя.

  Оболочка Bash или Korn:

  Добавьте в файл *домашний_каталог_пользователей_экземпляра*/sqllib/userprofile следующую запись (в одной строке):

  ```
  export LD_LIBRARY_PATH=каталог_bin_сервера/
  dbbkapi:/usr/local/ibm/gsk8_64/lib64:
  /opt/ibm/lib:
  /opt/ibm/lib64:$LD_LIBRARY_PATH
  ```

  Оболочка C:

  Добавьте в файл *домашний_каталог_пользователей_экземпляра*/sqllib/usercshrc следующую запись (на одной строке):

  ```
  setenv LD_LIBRARY_PATH каталог_bin_сервера/dbbkapi:/
  usr/local/ibm/gsk8_64/lib64:/
  opt/ibm/lib:/opt/ibm/lib64:/usr/lib64:$LD_LIBRARY_PATH
  ```

  Напоминание: В пути библиотек должны быть следующие записи, и они должны идти перед всеми другими записями в пути библиотек:

  – каталог_bin_сервера/dbbkapi

  – /usr/local/ibm/gsk8_64/lib64

4. Создайте новый файл серверных опций.

Конфигурирование связи между сервером и клиентом

Пример файла серверных опций по умолчанию, dsmserv.opt.smp, создается в каталоге /opt/tivoli/tsm/server/bin при установке IBM Spectrum Protect. Вы должны сконфигурировать связь между сервером и клиентами, создав новый файл серверных опций. Для этого скопируйте пример файла в каталог экземпляра сервера.

Об этой задаче

Убедитесь, что у вас есть каталог экземпляра сервера, например, /tsminst1, и скопируйте в него файл примера. Присвойте новому файлу имя dsmserv.opt и измените опции. Выполните это действие до инициализации базы данных сервера. Каждый образец записи или запись по

умолчанию в стандартном файле опций является примечанием - строкой, начинающейся со звездочки (*). Регистр символов в именах опций не имеет значения, а между ключевыми словами и значениями можно вставлять один или несколько пробелов.

При изменении файла опций соблюдайте следующие рекомендации.

- Для активации опции удалите звездочку в начале строки.
- Для ввода опций можно использовать любой столбец.
- Одна строка должна содержать только одну опцию, а одна опция должна занимать только одну строку.
- Если одному ключевому слову соответствует несколько записей, сервер IBM Spectrum Protect использует последнюю запись.

При внесении изменений в файл опций сервера необходимо перезапустить сервер, чтобы изменения вступили в силу.

Можно задать один из следующих методов связи:

- TCP/IP версии 4 или версии 6
- Совместное использование памяти
- Secure Sockets Layer (SSL)

  Совет: Пароли можно аутентифицировать с помощью сервера каталогов LDAP или сервера IBM Spectrum Protect. Пароли, которые аутентифицированы с помощью сервера каталогов LDAP, могут обеспечить расширенную защиту системы.

Задание опций TCP/IP

Задайте опции TCP/IP для сервера IBM Spectrum Protect или сохраните опции, выбранные по умолчанию.

Об этой задаче

Ниже приводится пример списка опций TCP/IP, которые вы можете использовать для конфигурирования системы.

```
commmethod        tcpip
  tcpport           1500
  tcpwindowsize   0
  tcpnodelay      yes
```

Совет: Можно использовать протокол TCP/IP версии 4, версии 6 или обеих версий.

TCPPORT
Адрес порта сервера для взаимодействий TCP/IP и SSL. Значение по умолчанию - 1500.

TCPWINDOWSIZE
Задает размер буфера TCP/IP, используемого при отправке или приеме данных. Размер окна, используемого в сеансе, меньше размера окна для сервера и клиента. При большем размере окна используется дополнительная память, но это может способствовать повышению производительности.

Можно задать целое число от 0 до 2048. Чтобы использовать размер окна по умолчанию для операционной системы, задайте значение 0.

TCPNODELAY
Позволяет указать, будет ли сервер отправлять сообщения малого объема, или же он разрешит TCP/IP буферизовать сообщения. При отправке небольших сообщений может повыситься пропускная способность, но при этом увеличится число пакетов, отправляемых по сети. Укажите YES, чтобы отправлять короткие сообщения, или NO, чтобы протокол TCP/IP сохранял их в буфере. Значение по умолчанию - YES.

TCPADMINPORT
Задает номер порта, который используется драйвером связи TCP/IP сервера для ожидания требований связи с поддержкой TCP/IP или SSL, отличных от сеансов клиентов. Значением по умолчанию является значение TCPPORT.

SSLTCPPORT
(Только SSL) Задает номер порта Secure Sockets Layer (SSL), на котором драйвер связи TCP/IP ожидает запросы на установление сеансов SSL от клиента резервного копирования и архивирования и клиента администрирования с интерфейсом командной строки.

SSLTCPADMINPORT
(Только SSL) Задает адрес порта, на котором драйвер связи TCP/IP сервера ожидает запросов на установление сеансов SSL от клиента администрирования с интерфейсом командной строки.

Задание опций Shared Memory

Вы можете использовать связь через совместную память (Shared Memory) для взаимодействия между клиентами и серверами на одном и том же компьютере. Чтобы использовать способ связи Shared Memory, в системе должен быть установлен протокол TCP/IP версии 4.

Об этой задаче

В приведенном ниже примере показан параметр для совместно используемой памяти (shared memory):

```
commmethod     sharedmem
   shmport     1510
```

В этом примере **SHMPORT** задает адрес порта TCP/IP для сервера при связи через совместно используемую память. Опцию **SHMPORT** можно использовать, чтобы задать другой порт TCP/IP. По умолчанию используется порт 1510.

COMMMETHOD можно использовать несколько раз в файле опций сервера IBM Spectrum Protect с различными значениями. Например, можно задать значения так:

```
commmethod        tcpip
commmethod     sharedmem
```

При использовании связи через совместную память вы можете получить от сервера следующее сообщение:

```
ANR9999D shmcomm.c(1598): ThreadId<39>
Error from msgget (2), errno = 28
```

Это сообщение означает, что необходимо создать очередь сообщений, но при этом будет превышено максимально допустимое число очередей сообщений (**MSGMNI**).

Чтобы узнать максимальное число очередей сообщений (**MSGMNI**) в системе, введите следующую команду:

```
cat /proc/sys/kernel/msgmni
```

Чтобы увеличить значение **MSGMNI** в системе, введите следующую команду:

```
sysctl -w kernel.msgmni=n
```

где **n** - максимальное число очередей сообщений в системе (MSGMNI), которое вы хотите задать.

Задание опций Secure Sockets Layer

Можно добавить дополнительную защиту данных и паролей с помощью протокола Secure Sockets Layer (SSL).

Прежде чем начать

SSL — это стандартная технология создания зашифрованных сеансов между серверами и клиентами. SSL предоставляет безопасный канал для связи серверов и клиентов по открытым путям связи. При использовании SSL идентификационная информация сервера проверяется с помощью цифровых сертификатов.

Чтобы обеспечить оптимальную производительность системы, используйте SSL только для сеансов, где это необходимо. Добавьте на сервер IBM Spectrum Protect дополнительные ресурсы процессора, чтобы удовлетворить возросшие требования.

Форматирование базы данных и журнала

Если вы конфигурируете сервер вручную, то надо сформатировать базу данных сервера и журнал восстановления. База данных используется для хранения информации о клиентских данных и серверных операциях, а журнал восстановления можно использовать для восстановления после сбоев системы и носителей. Воспользуйтесь утилитой **DSMSERV FORMAT** для форматирования и инициализации базы данных сервера и журнала восстановления. При инициализации базы данных и журнала восстановления запрещаются все прочие операции сервера.

После конфигурирования связей сервера все готово для инициализации базы данных. Каталоги не должны находиться в файловых системах, где может закончиться свободное пространство. Если некоторые каталоги, например, архивный журнал, больше не доступны или переполнены, сервер прекратит работу. Дополнительные сведения смотрите в разделе Планирование емкости.

Как настроить обработчик списков завершения работы

Задайте для переменной реестра **DB2NOEXITLIST** значение ON для каждого экземпляра сервера. Войдите в систему, используя ID пользователя экземпляра, и введите следующую команду:

```
db2set -i имя_экземпляра_сервера
DB2NOEXITLIST=ON
```

Например:

```
db2set -i tsminst1 DB2NOEXITLIST=ON
```

Инициализация базы данных сервера и журнала восстановления

Используйте утилиту **DSMSERV FORMAT** для форматирования и инициализации базы данных сервера, которая является базой данных IBM Db2, и журнала восстановления. Например, если каталог экземпляра сервера - это */tsminst1*, то введите следующие команды:

```
cd /tsminst1
dsmserv format dbdir=/tsmdb001 activelogsize=32768
activelogdirectory=/activelog archlogdirectory=/archlog
archfailoverlogdirectory=/archfaillog mirrorlogdirectory=/mirrorlog
```

Совет: Если вы зададите несколько каталогов, убедитесь, что размеры соответствующих файловых систем равны, что позволит обеспечить непротиворечивую 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.

Если база данных Db2 не запускается после выполнения команды **DSMSERV FORMAT**, то, возможно, придется выключить опцию монтирования файловой системы NOSUID. Опцию надо выключить, чтобы запустить систему, в следующих случаях:

- Если эта опция задана в файловой системе, содержащей каталог владельца экземпляра Db2.
- Если опция задана для какой-либо файловой системы, содержащей базу данных, активные журналы, архивные журналы, журналы отказоустойчивости или зеркалированные журналы Db2.

После отключения опции NOSUID повторите монтирование файловой системы и запустите базу данных Db2, введя следующую команду:

```
db2start
```

Создание администратора

После завершения форматирования базы данных и журнала восстановления надо создать пользователя-администратора, который сможет войти на сервер, а также включить IBM Spectrum Protect Operations Center для соединения с сервером. Для настройки пользователя-администратора можно использовать следующие команды в макросе:

REGISTER ADMIN
Команда **REGISTER ADMIN** принимает следующие параметры:

```
register admin ID_администратора пароль_администратора
```

Длина пароля должна соответствовать определенным правилам. Дополнительную информацию смотрите в разделе REGISTER ADMIN (зарегистрировать ID администратора)

GRANT AUTH
Команда **GRANT AUTH** принимает следующие параметры:

```
grant auth ID_администратора classes=класс_администратора
```

Дополнительную информацию смотрите в разделе GRANT AUTHORITY (Добавить полномочия администратора).

Чтобы настроить пользователя-администратора, выполните следующее:

1. Создайте макрос, например, `setup.mac`.
2. Отредактируйте макрос, чтобы зарегистрировать пользователя-администратора и предоставить системные полномочия пользователю со следующими идентификационными данными:
   - ID пользователя-администратора: `adminadmin`
   - Пароль для пользователя-администратора: `adminadmin1`

   ```
   register admin adminadmin adminadmin1
   grant auth adminadmin classes=system
   ```

   Надо создать пользователя-администратора с помощью опции **classes=system**, чтобы пользователь-администратор мог создавать других потенциальных пользователей-администраторов, например, с ограниченными полномочиями. После этого любой из этих администраторов сможет подключаться к IBM Spectrum Protect Operations Center.
3. Чтобы создать пользователя-администратора и предоставить ему системные полномочия, введите команду **DSMSERV** с опцией **runfile** и файлом макроса, например:

   ```
   dsmserv runfile setup.mac
   ```

После этого администратор может запустить экземпляр сервера и соединиться с сервером, чтобы выполнить другие необходимые шаги, например, настроить резервную копию базы данных.

Подготовка менеджера базы данных к резервному копированию базы данных

Чтобы создать резервную копию данных в базе данных для IBM Spectrum Protect, нужно разрешить менеджер базы данных и сконфигурировать интерфейс прикладного программирования (Application Programming Interface - API) IBM Spectrum Protect.

Об этой задаче

Начиная с IBM Spectrum Protect V7.1.1 больше нет необходимости задавать пароль API во время конфигурирования сервера вручную. Если задать пароль API в процессе конфигурирования вручную, то попытки резервного копирования базы данных могут завершиться неудачно.

Если вы создаете экземпляр сервера IBM Spectrum Protect при помощи мастера по конфигурированию, то вам не нужно выполнять эти действия. Если вы конфигурируете экземпляр вручную, выполните описанные ниже шаги, прежде чем вводить команду **BACKUP DB** или **RESTORE DB**.

Внимание: Если база данных недоступна, весь сервер IBM Spectrum Protect становится недоступным. Если база данных утеряна и ее нельзя восстановить, может оказаться затруднительным или даже невозможным восстановить данные, которыми управляет этот сервер. Поэтому очень важно создать резервную копию базы данных.

В следующих командах замените значения из примера фактическими значениями. В примерах используется значение `tsminst1` в качестве ID пользователя экземпляра сервера, `/tsminst1` в качестве каталога экземпляра сервера и `/home/tsminst1` в качестве домашнего каталога пользователя экземпляра сервера.

1. Задайте конфигурацию переменных среды API IBM Spectrum Protect для экземпляра базы данных:
   a. Войдите в систему от имени ID пользователя `tsminst1`.
   b. После входа пользователя `tsminst1` в систему убедитесь, что среда IBM Db2 правильно инициализирована. Среда Db2 инициализируется путем запуска сценария `/home/tsminst1/sqllib/db2profile`, который обычно запускается автоматически из профиля ID пользователя. Убедитесь, что в домашнем каталоге пользователя экземпляра существует файл `.profile`, например, `/home/tsminst1/.profile`. Если `.profile` не запускает сценария `db2profile` добавьте в него следующие строки:

```
if [ -f /home/tsminst1/sqllib/db2profile ]; then
      . /home/tsminst1/sqllib/db2profile
  fi
```

   c. Добавьте в файл `каталог_экземпляра/sqllib/userprofile` следующие строки:

```
DSMI_CONFIG=каталог_экземпляра_сервера/tsmdbmgr.opt
DSMI_DIR=каталог_bin_сервера/dbbkapi
DSMI_LOG=каталог_экземпляра_сервера
export DSMI_CONFIG DSMI_DIR DSMI_LOG
```

   Здесь используются следующие обозначения:

   - *каталог_экземпляра* - это домашний каталог пользователя экземпляра сервера.
   - *каталог_экземпляра_сервера* - это каталог экземпляра сервера.
   - *каталог_сервера_bin* - это каталог bin сервера. Каталог по умолчанию - `/opt/tivoli/tsm/server/bin`.

   Добавьте в файл `каталог_экземпляра/sqllib/usercshrc` следующие строки:

```
setenv DSMI_CONFIG=каталог_экземпляра_сервера/tsmdbmgr.opt
setenv DSMI_DIR=каталог_bin_сервера/dbbkapi
setenv DSMI_LOG=каталог_экземпляра_сервера
```

2. Выйдите из системы и снова войдите в нее от имени `tsminst1` либо введите команду:

```
. ~/.profile
```

Совет: Убедитесь, что после начальной точки (.) введен пробел.

3. Создайте файл с именем `tsmdbmgr.opt` в каталоге *экземпляр_сервера*, который в этом примере находится в каталоге `/tsminst1`, и добавьте в него следующую строку:

```
SERVERNAME TSMDBMGR_TSMINST1
```

Напоминание: Значение SERVERNAME должно совпадать в файлах `tsmdbmgr.opt` и `dsm.sys`.

4. От имени пользователя root добавьте в файл конфигурации API IBM Spectrum Protect `dsm.sys` указанные ниже строки. По умолчанию файл конфигурации `dsm.sys` находится в следующем каталоге:

   каталог_сервера_bin`/dbbkapi/dsm.sys`

```
servername TSMDBMGR_TSMINST1
commmethod         tcpip
tcpserveraddr localhost
tcpport            1500
errorlogname /tsminst1/tsmdbmgr.log
nodename $$_TSMDBMGR_$$
```

   где

   - *servername* соответствует значению `servername` в файле `tsmdbmgr.opt`.
   - *commethod* задает API клиента, используемый для связи с сервером при резервном копировании базы данных. Это может быть значение `tcpip` или `sharedmem`. Дополнительную информацию о совместно используемой памяти смотрите в описании шага 5.
   - *tcpserveraddr* задает адрес сервера, который API клиента будет использовать для связи с сервером для резервного копирования базы данных. Для резервного копирования базы данных надо задать значение `localhost`.

     Важное замечание: Если ваш сервер использует сертификат, подписанный сертификатором, то надо указать внешний IP-адрес сервера для опции *tcpserveraddr*.
   - *tcpport* задает номер порта, который API клиента будет использовать для связи с сервером с целью резервного копирования базы данных. Значение `tcpport` должно быть значением, которое задано в файле опций сервера `dsmserv.opt`.
   - *errorlogname* задает журнал ошибок, в который API клиента будет записывать ошибки, происходящие при резервном копировании базы данных. Обычно этот журнал находится в каталоге экземпляра сервера. Однако его можно поместить в любой другой каталог, разрешения на запись в который есть у ID пользователя.
   - *nodename* задает имя узла, которое API клиента будет использовать для соединения с сервером при резервном копировании базы данных. Чтобы обеспечить возможность резервного копирования базы данных, нужно задать значение `$$_TSMDBMGR_$$`.

   Внимание: Не добавляйте в опцию PASSWORDACCESS `generate` в файл конфигурации `dsm.sys`. Эта опция может привести к сбою резервного копирования базы данных.

5. Необязательно: Сконфигурируйте сервер для резервного копирования базы данных с использованием совместно используемой памяти. Таким образом вы можете уменьшить нагрузку на процессор и увеличить пропускную способность. Выполните следующие шаги:

   a. Просмотрите файл `dsmserv.opt`. Если следующие строки отсутствуют в этом файле, то добавьте их:

```
commmethod     sharedmem
shmport номер_порта
```

      где *номер_порта* задает порт, используемый для совместно используемой памяти.

   b. В файле конфигурации `dsm.sys` найдите следующие строки:

```
commmethod         tcpip
tcpserveraddr localhost
tcpport номер_порта
```

Замените указанные строки следующими строками:

```
commmethod      sharedmem
shmport номер_порта
```

где *номер_порта* задает порт, используемый для совместно используемой памяти.

Опции конфигурирования сервера для обслуживания сервера баз данных

Чтобы избежать проблем с ростом базы данных и производительности сервера, сервер автоматически отслеживает таблицы своих баз данных и реорганизует их по мере надобности. Перед переводом сервера в производственный режим задайте опции сервера, управляющие временем реорганизации. Если вы собираетесь использовать дедупликацию данных, убедитесь, что включена опция запуска реорганизации индексов.

Об этой задаче

Для реорганизации таблиц и индексов требуются значительные процессорные ресурсы, пространство для активного журнала и пространство для архивного журнала. Поскольку резервное копирование баз данных имеет приоритет перед реорганизацией, выберите время и длительность для реорганизации так, чтобы эти процессы не перекрывались и реорганизация смогла завершиться.

Вы можете оптимизировать реорганизацию индекса и таблиц для базы данных сервера. Таким образом можно избежать неожиданного роста базы данных и проблем, отрицательно влияющих на производительность. Инструкции смотрите в техническом примечании 1683633.

Если вы изменяете эти опции сервера при работающем сервере, надо остановить и перезапустить сервер, чтобы они вступили в силу.

Процедура

1. Измените опции сервера.

   Отредактируйте файл опций сервера `dsmserv.opt` в каталоге экземпляра сервера. При изменении файла опций сервера придерживайтесь следующих рекомендаций:

   - Чтобы включить опцию, удалите звездочку в начале строки.
   - Введите опцию в любой строке.
   - Вводите по одной опции на строке. Вся опция со своим значением должна быть записана на одной строке.
   - Если для одной опции в файле есть несколько записей, сервер использует последнюю запись.

   Чтобы просмотреть доступные опции сервера, воспользуйтесь файлом примера `dsmserv.opt.smp` в каталоге `/opt/tivoli/tsm/server/bin`.
2. Если вы собираетесь использовать дедупликацию данных, то разрешите опцию сервера **ALLOWREORGINDEX**.

   Добавьте следующую опцию и значение в файл опций сервера:

   ```
   allowreorgindex yes
   ```
3. Задайте опции сервера **REORGBEGINTIME** и **REORGDURATION**, управляющие моментом начала реорганизации и ее длительностью. Выберите время и длительность, чтобы выполнять реорганизацию во время ожидаемой минимальной занятости сервера.

   Эти опции сервера действуют на процессы реорганизации как таблиц, так и индексов.

   a) Задайте время начала реорганизации при помощи опции сервера **REORGBEGINTIME**. Задайте время по 24-часовой системе.
   Например, чтобы начать реорганизацию в 8.30 вечера, задайте в файле опций сервера:

```
reorgbegintime 20:30
```

b) Задайте интервал, в который сервер может начать реорганизацию.
Например, чтобы указать, что сервер может начать реорганизацию в течении четырех часов после времени, заданного опцией сервера **REORGBEGINTIME**, задайте в файле опций сервера:

```
reorgduration 4
```

4. Если в момент изменения файла опций сервера сервер работает, остановите и перезапустите его.

Запуск экземпляра сервера

Сервер можно запускать от имени ID пользователя экземпляра (что является предпочтительным методом) или от имени ID пользователя root.

Прежде чем начать

Убедитесь, что вы правильно задали разрешения и пределы пользователя.

Об этой задаче

При запуске сервера с использованием ID пользователя экземпляра упрощается процесс конфигурирования и исключаются потенциальные проблемы. Однако в некоторых случаях может потребоваться запуск сервера под ID пользователя root. Например, вы можете захотите использовать ID пользователя root, чтобы сервер мог обращаться к определенным устройствам. Можно настроить автоматический запуск сервера, используя либо ID пользователя экземпляра, либо ID пользователя root.

Если вам нужно выполнить задачи по обслуживанию или переконфигурированию, запустите сервер в режиме обслуживания.

Процедура

Чтобы запустить сервер, выполните одно из следующих действий:

- Запустите сервер от имени ID пользователя экземпляра.

  Инструкции смотрите в разделе “Запуск сервера от имени ID пользователя экземпляра” на стр. 107.
- Запустите сервер от имени ID пользователя root.

  Инструкции по авторизации ID пользователей root для запуска сервера смотрите на веб-странице Авторизация ID пользователей root для запуска сервера (V7.1.1). Инструкции по запуску сервера с ID пользователя root смотрите на веб-странице Запуск сервера от имени ID пользователя root (V7.1.1).
- Автоматический запуск сервера.

  Инструкции смотрите в разделе “Автоматический запуск серверов в системах Linux” на стр. 108.
- Запустите сервер в режиме обслуживания.

  Инструкции смотрите в разделе “Запуск сервера в режиме обслуживания” на стр. 109.

Проверка прав доступа и ограничений для пользователей

Перед запуском сервера проверьте права доступа и пределы пользователя.

Об этой задаче

Если не проверить пользовательские пределы (другое название - *значения ulimit*, могут возникнуть нестабильность или ошибки ответов сервера. Нужно также проверить предел для максимального числа открытых файлов, установленный на уровне системы. Этот предел на уровне системы не может быть меньше пользовательского предела.

Процедура

1. Убедитесь, что у ID пользователя экземпляра сервера есть разрешения на запуск сервера.
2. Для экземпляра сервера, который вы собираетесь запускать, убедитесь, что у вас есть полномочия на чтение и запись файлов в каталоге этого экземпляра сервера.

   Проверьте, что в каталоге экземпляра сервера существует файл `dsmserv.opt` и он включает в себя параметры для экземпляра сервера.
3. Если сервер подключается к ленточному накопителю, чейнджеру носителей или устройству со сменными носителями, а вы собираетесь запускать сервер под ID пользователя экземпляра сервера, предоставьте этому ID пользователя доступ на чтение и запись для указанных устройств. Чтобы задать разрешения, выполните одно из следующих действий:

   - Если система выделена для IBM Spectrum Protect и доступ есть только у администратора IBM Spectrum Protect, задайте для специального файла устройства общий доступ с правом записи. Введите в командной строке операционной системы следующую команду:

     ```
     chmod +w /dev/rmtX
     ```

   - Если в системе несколько пользователей, вы можете ограничить доступ, сделав ID пользователя экземпляра IBM Spectrum Protect владельцем специальных файлов устройств. Введите в командной строке операционной системы следующую команду:

     ```
     chmod u+w /dev/rmtX
     ```

   - Если на одном и том же компьютере работают экземпляры нескольких пользователей, измените имя группы, например, TAPEUSERS, и добавьте в эту группу каждый ID пользователя экземпляра IBM Spectrum Protect. Затем измените для специальных файлов устройств владельца, так чтобы их владельцем стала группа TAPEUSERS, и предоставьте группе разрешение на запись этих файлов. Введите в командной строке операционной системы следующую команду:

     ```
     chmod g+w /dev/rmtX
     ```
4. Если используется драйвер устройств IBM Spectrum Protect и утилита **autoconf**, предоставьте при помощи опции **-a** доступ с правом чтения/записи этому ID пользователя экземпляра.
5. Чтобы предотвратить отказы сервера при взаимодействии с IBM Db2, настройте параметры ядра.

   Инструкции о настройке параметров ядра смотрите в разделе Настройка параметров ядра.
6. Проверьте следующие пределы пользователя на соответствие рекомендациям в таблице.

Таблица 20. Значения пользовательского предела (ulimit)

Тип пользовательского предела	Рекомендуемое значение	Команда для запроса значения
Максимальный размер создаваемых файлов ядра	Без ограничений	`ulimit -Hc`
Максимальный размер сегмента данных для процесса	Без ограничений	`ulimit -Hd`
Максимальный размер файлов	Без ограничений	`ulimit -Hf`

Таблица 20. Значения пользовательского предела (ulimit) (продолжение)

Тип пользовательского предела	Рекомендуемое значение	Команда для запроса значения
Максимальное число открытых файлов	65536	`ulimit -Hn`
Максимальное время процессора в секундах	Без ограничений	`ulimit -Ht`

Чтобы изменить пользовательские пределы, выполните инструкции в документации к используемой операционной системе.

Совет: Если вы собираетесь запускать сервер автоматически при помощи сценария, пользовательские пределы можно задать в этом сценарии.

7. Убедитесь, что для пользовательского предела максимального числа пользовательских процессов (`параметр nproc`) задано минимальное рекомендуемое значение 16384.
   a) Для проверки текущего пользовательского значения введите команду`ulimit -Hu` от имени ID пользователя экземпляра.
   Например:

   ```
   [user@Machine ~]$ ulimit -Hu
   16384
   ```

   b) Если предел максимального числа пользовательских процессов не равен 16384, то задайте значение 16384.

   Добавьте следующую строку в файл `/etc/security/limits.conf`:

   ```
   ID_пользователя_экземпляра         -    nproc           16384
   ```

   где *ID_пользователя_экземпляра* - это ID пользователя экземпляра сервера.

   Если сервер установлен в операционной системе Red Hat Enterprise Linux 6, задайте пользовательский предел, отредактировав файл `/etc/security/limits.d/90-nproc.conf` в каталоге `/etc/security/limits.d`. Этот файл перезаписывает значения в файле `/etc/security/limits.conf`.

   Совет: Предельное значение по умолчанию для максимального числа пользовательских процессов изменено в некоторых дистрибутивах и версиях операционной системы Linux. Значение по умолчанию - 1024. Если не изменить это значение на минимальное предлагаемое значение 16384, возможны отказы и зависания сервера.

Запуск сервера от имени ID пользователя экземпляра

Чтобы запустить сервер под ID пользователя экземпляра, войдите в систему с ID пользователя root и введите в каталоге экземпляра сервера соответствующую команду.

Прежде чем начать

Убедитесь, что права доступа и пределы пользователей заданы правильно.

Процедура

1. Войдите в систему, в которой установлен IBM Spectrum Protect, от имени ID пользователя экземпляра для сервера.
2. Если у вас нет профиля пользователя, который запускает сценарий `db2profile`, то введите следующую команду:

   ```
   . /home/tsminst1/sqllib/db2profile
   ```

Совет: Инструкции об изменении сценария входа в систему ID пользователя для автоматического запуска сценария db2profile смотрите в разделе Информация о продукте Db2.

3. Запустите сервер, введя следующую команду в одной строке из каталога экземпляра сервера:

```
usr/bin/dsmserv
```

Совет: Эта команда выполняется в режиме активного окна, так что вы сможете задать ID администратора и соединиться с экземпляром сервера.

Например, если имя экземпляра сервера - tsminst1, а каталог экземпляра сервера - /tsminst1, введите следующие команды:

```
cd /tsminst1
 . ~/sqllib/db2profile
/usr/bin/dsmserv
```

Автоматический запуск серверов в системах Linux

Используйте для автоматического запуска сервера в Linux сценарий **dsmserv.rc**.

Прежде чем начать

Убедитесь, что правильно заданы параметры ядра.

Убедитесь в том, что экземпляр сервера запущен от имени ID пользователя владельца экземпляра.

Убедитесь, что права доступа и пределы пользователей заданы правильно.

Об этой задаче

Сценарий **dsmserv.rc** расположен в каталоге установки сервера, например, /opt/tivoli/tsm/server/bin.

Сценарий **dsmserv.rc** можно использовать для запуска сервера вручную или же автоматически, если добавить записи в каталог /etc/rc.d/init.d. Этот сценарий работает с утилитами Linux, такими как **CHKCONFIG** и **SERVICE**.

Процедура

Для каждого экземпляра сервера, который вы хотите запускать автоматически, выполните следующие действия:

1. Поместите копию сценария **dsmserv.rc** в каталог /init.d, например, в /etc/rc.d/init.d.

   Убедитесь, что вы изменяете только копию сценария. Не изменяйте исходный сценарий.

2. Переименуйте копию сценария, чтобы она соответствовала владельцу экземпляра сервера, например: tsminst1.

   В созданном сценарии предполагается, что каталог экземпляра сервера - *домашний_каталог*/tsminst1, например: /home/tsminst1/tsminst1.

3. Если каталог экземпляра сервере - не *домашний_каталог*/tsminst1, найдите в копии сценария следующую строку:

   ```
   instance_dir="${instance_home}/tsminst1"
   ```

   Измените эту строку так, чтобы она указывала на используемый каталог экземпляра сервера, например:

   ```
   instance_dir="/tsminst1"
   ```

4. Найдите в копии сценария следующую строку:

```
# pidfile: /var/run/dsmserv_instancename_su.pid
```

Замените имя экземпляра на имя владельца экземпляра сервера.

Например, если имя владельца экземпляра tsminst1, то измените строку так:

```
# pidfile: /var/run/dsmserv_tsminst1_su.pid
```

5. Сконфигурируйте уровень выполнения, на котором должен автоматически запускаться сервер. При помощи таких инструментов, как утилита **CHKCONFIG**, задайте значение, соответствующее многопользовательскому режиму с включенной поддержкой работы по сети. Как правило, используется уровень выполнения 3 или 5, в зависимости от операционной системы и ее конфигурации. Дополнительную информацию о многопользовательском режиме и уровнях выполнения смотрите в документации для используемой операционной системы.
6. Чтобы запустить или остановить сервер, введите одну из следующих команд:
   - Чтобы запустить сервер:

     ```
     service tsminst1 start
     ```

   - Чтобы остановить сервер:

     ```
     service tsminst1 stop
     ```

Пример

В этом примере используются следующие значения:

- Владелец экземпляра - tsminst1.
- Каталог экземпляра сервера - `/home/tsminst1/tsminst1`.
- Имя копии сценария **dsmserv.rc** - `tsminst1`.
- Для конфигурирования запуска сценария с уровнями выполнения 3, 4 и 5 используется утилита **CHKCONFIG**.

```
cp /opt/tivoli/tsm/server/bin/dsmserv.rc /etc/rc.d/init.d/tsminst1
sed -i 's/dsmserv_instancename.pid/dsmserv_tsminst1.pid/' /etc/rc.d/init.d/tsminst1
chkconfig --list tsminst1
service tsminst1 supports chkconfig, but is not referenced in   /*служба tsminst1 поддерживает
chkconfig, но на нее нет ссылок)*/
any runlevel (run 'chkconfig --add tsminst1')   /*ни на одном уровне выполнения (запустите
'chkconfig --add tsminst1')*/
chkconfig --add tsminst1
chkconfig --list tsminst1
tsminst1 0:off 1:off 2:off 3:off 4:off 5:off 6:off
chkconfig --level 345 tsminst1 on
chkconfig --list tsminst1
tsminst1 0:off 1:off 2:off 3:on 4:on 5:on 6:off
```

Запуск сервера в режиме обслуживания

Сервер можно запустить в режиме обслуживания, чтобы избежать повреждений при выполнении задач по обслуживанию и переконфигурированию.

Об этой задаче

Запустите сервер в режиме обслуживания, запустив утилиту **DSMSERV** с параметром **MAINTENANCE**.

В режиме обслуживания отключаются следующие операции:

- Расписания 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, `dsmserv.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:

  ```
  dsmserv 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.

Операции, которые были отключены во время режима обслуживания, будут снова включены.

Остановка сервера

При необходимости сервер можно остановить, чтобы передать управление операционной системе. Чтобы предотвратить отключение административных и клиентских узлов, останавливайте сервер только после завершения или отмены текущих сеансов.

Об этой задаче

Чтобы остановить сервер, введите в командной строке IBM Spectrum Protect следующую команду:

```
halt
```

Если невозможно подключиться к серверу в качестве клиента администрирования, но нужно остановить сервер, следует отменить процесс с помощью команды **kill** с указанием идентификационного номера (pid) процесса. Значение pid будет показано при инициализации.

Важное замечание: Перед тем, как ввести команду **kill**, убедитесь что вам известен правильный идентификатор сервера IBM Spectrum Protect.

Для определения номера процесса, который нужно выгрузить, можно использовать файл `dsmserv.v6lock` в том каталоге, из которого запущен сервер. Чтобы увидеть файл, введите:

```
cat /instance_dir/dsmserv.v6lock
```

Чтобы остановить сервер, введите следующую команду:

```
kill -23 dsmserv_pid
```

где *dsmserv_pid* - это числовой ID процесса.

Регистрация лицензий

Сразу же зарегистрируйте все лицензированные функции IBM Spectrum Protect, которые вы приобрели, чтобы не потерять никаких данных после начала выполнения сервером таких операций, как резервное копирование ваших данных.

Об этой задаче

Используйте для этого команду **REGISTER LICENSE**.

Пример: зарегистрировать лицензию

Зарегистрируйте базовую лицензию на IBM Spectrum Protect.

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

Подготовка сервера к операциям резервного копирования базы данных

Чтобы подготовить сервер к автоматическим и ручным операциям резервного копирования базы данных, убедитесь, что вы указали класс ленточных, файловых или облачных устройств, а также выполнили другие шаги.

Процедура

1. Убедитесь, что конфигурация сервера IBM Spectrum Protect - полная.

   Совет: Сервер можно сконфигурировать для резервного копирования базы данных, используя мастер конфигурирования (`dsmicfgx`), или можно выполнить эти шаги вручную. Дополнительную информацию о конфигурации смотрите в разделе *Конфигурирование серверов* в IBM Knowledge Center.
2. Выберите класс устройств, который следует использовать для резервного копирования базы данных, защитите главный ключ шифрования и задайте пароль.

   Убедитесь, что следующие файлы ключей защищены:

   - Файлы главного ключа шифрования (dsmkeydb.*)
   - Сертификат сервера и файлы секретных ключей (cert.*)

   Чтобы выполнить эти действия, введите команду **SET DBRECOVERY** из административной командной строки:

   ```
   set dbrecovery имя_класса_устройств protectkeys=yes password=имя_пароля
   ```

   где *имя_класса_устройств* задает класс устройств, который следует использовать для операций резервного копирования базы данных, а *имя_пароля* задает пароль.

   Вы обязательно должны задать имя класса устройств, иначе резервное копирование завершится неудачно. Задав **PROTECTKEYS=YES**, вы сделаете так, что во время операций резервного копирования базы данных будет создаваться резервная копия главного ключа шифрования. Для класса облачных устройств требуется параметр **PROTECTKEYS=YES**.

   Создайте надежный пароль, содержащий хотя бы 8 символов. Если задан пароль для резервной копии базы данных, вы должны указать тот же самый пароль в команде **RESTORE DB** для восстановления базы данных.

   Внимание: Убедитесь, что вы помните пароль, и сохраните копию в защищенном положении. Без пароля данные нельзя восстановить.

Пример

Чтобы указать, что резервные копии базы данных содержат копию главного ключа шифрования для сервера, введите следующую команду:

```
set dbrecovery dbback protectkeys=yes password=protect8991
```

Запуск нескольких экземпляров серверов на одном компьютере

Вы можете создать несколько экземпляров сервера в системе. У каждого экземпляра сервера будет свой отдельный каталог экземпляра и свои отдельные каталоги базы данных и журнала.

Умножьте требования к памяти и другим системным ресурсам для одного сервера на число экземпляров, которые вы собираетесь создать в системе.

Набор файлов для одного экземпляра сервера хранится отдельно от файлов, используемым другим экземпляром сервера в той же системе. Выполните действия, описанные в разделе раздел Создание экземпляра сервера для каждого нового экземпляра, включая создание нового пользователя экземпляра.

Чтобы управлять объемом системной памяти, используемым каждым сервером, задайте опцию DBMEMPERCENT, позволяющую ограничить процент системной памяти. Если все серверы равноценны, используйте для всех серверов одинаковые значения. Если один сервер является производственным сервером, а остальные серверы являются тест-серверами, задайте для производственного сервера более высокое значение, чем для тест-серверов.

Можно произвести обновление V7.1 до V8.1 напрямую. Дополнительную информацию смотрите в разделе обновления. Если при обновлении в вашей системе есть несколько серверов, запускать мастер установки нужно только один раз. Мастер установки соберет информацию о базах данных и переменных для всех исходных экземпляров сервера.

Мониторинг сервера

Когда вы начнете использовать сервер в производственном режиме, отслеживайте пространство, используемое сервером, чтобы убедиться, что объем пространства достаточен. Если нужно, то настройте пространство.

Процедура

1. Следите за активным журналом, чтобы убедиться, что его размер соответствует рабочей нагрузке, обрабатываемой экземпляром сервера.

   Если уровень рабочей нагрузки на сервер приближается к типичному ожидаемому уровню, то объем пространства, используемого активным журналом, составляет 80-90% пространства. В этот момент, возможно, нужно увеличить объем пространства. Необходимость увеличения пространства зависит от типов транзакций, составляющих рабочую нагрузку сервера. Характеристики транзакций влияют на то, как используется пространство активного журнала.

   На использованием пространства активного журнала могут влиять следующие характеристики транзакций:

   - Число и размер файлов в операциях резервного копирования.
     - Такие клиенты, как файл-серверы, которые создают резервные копии большого числа мелких файлов, могут инициировать большое число быстро завершающихся транзакций. Транзакции могут использовать большой объем пространства в активном журнале, но кратковременно.
     - Такие клиенты, как почтовый сервер или сервер базы данных, которые создают резервные копии больших объемов данных в ходе немногочисленных транзакций, могут инициировать небольшое число транзакций, для завершения которых требуется длительное время.

Транзакции могут использовать небольшой объем пространства в активном журнале, но в течение длительного времени.

- Типы соединений с сетью
  - Транзакции, связанные с операциями резервного копирования, которые выполняются с использованием высокоскоростных сетевых соединений, завершаются быстрее. Транзакции используют пространство в активном журнале в течение более короткого времени.
  - Для завершения транзакций, связанных с операциями резервного копирования, которые выполняются с использованием относительно низкоскоростных сетевых соединений, требуется больше времени. Транзакции используют пространство в активном журнале в течение более длительного времени.

Если сервер обрабатывает транзакции с широким диапазоном характеристик, то пространство, используемое для активного журнала, может значительно увеличиваться и уменьшаться с течением времени. В этом случае вы должны сделать так, чтобы, как правило, использовался меньший процент пространства активного журнала. Дополнительное пространство позволит активному журналу увеличиваться в размере, если для выполнения транзакций требуется очень много времени.

2. Следите за архивным журналом, чтобы убедиться в том, что для него всегда хватает места.

   Напоминание: Если архивный журнал и архивный журнал отказоустойчивости заполнятся, может заполниться активный журнал, и сервер остановится. Цель заключается в том, чтобы архивному журналу был доступен достаточный объем пространства и он никогда не использовал все доступное ему пространство.

   Вы, вероятно, заметите следующие закономерности:

   a. Сначала архивный журнал быстро растет по мере выполнения операций резервного копирования клиента.
   b. Резервное копирование базы данных производится регулярно либо по расписанию, либо вручную.
   c. После выполнения, как минимум, двух операций полного резервного копирования базы данных сокращение журналов происходит автоматически. В результате отбрасывания пространство, используемое архивным журналом, уменьшается.
   d. Обычные операции клиента продолжаются, и архивный журнал снова растет.
   e. Резервное копирование базы данных выполняется регулярно, и отбрасывание журналов происходит так же часто, как и операции полного резервного копирования базы данных.

   При таких закономерностях архивный журнал сначала растет, затем уменьшается, а затем может снова вырасти. С течением времени, по мере продолжения нормальной работы, объем пространства, используемого архивным журналом, должен достичь относительно постоянного уровня.

   Если архивный журнал продолжает расти, то выполните одно из описанных ниже действий или оба эти действия:

   - Добавьте пространство для архивного журнала. Это может означать перемещение архивного журнала в другую файловую систему.
   - Увеличьте частоту полного резервного копирования базы данных, чтобы отбрасывание журналов производилось чаще.

3. Если вы задали каталог для резервного архивного журнала, определите, сохраняются ли в этом каталоге какие-либо журналы при обычной работе. Если пространство резервного журнала используется, то увеличьте размер архивного журнала.

   Цель состоит в том, чтобы резервный архивный журнал использовался только в экстраординарных условиях, а не при обычной работе.

Глава 4. Установка пакета исправлений сервера IBM Spectrum Protect

Служебные обновления программного обеспечения IBM Spectrum Protect, также называемые пакетами Fix Pack, выводят сервер на текущий служебный уровень.

Прежде чем начать

Чтобы установить на сервер пакет Fix Pack или промежуточный пакет исправлений, установите сервер требуемого для выполнения уровня. Не обязательно запускать установку сервера на уровне базового выпуска. Например, если у вас установлена версия 8.1.1, то можно перейти сразу к самому последнему пакету Fix Pack для V8.1. Не обязательно начинать с установки V8.1.0, если доступно текущее изменение.

У вас должен быть установлен пакет лицензий IBM Spectrum Protect. Пакет лицензий приобретается вместе с базовым выпуском программного обеспечения. При загрузке пакета исправлений или промежуточного пакета исправлений с сайта Fix Central установите лицензию на сервер, которая есть на веб-сайте Passport Advantage. Для вывода сообщений и справки на языке, ином чем американский английский, установите языковый пакет по своему выбору.

Если вы обновляете сервер, а затем возвращаете сервер на более ранний уровень, то вы должны восстановить базу данных на момент времени перед обновлением. Во время процесса обновления выполните требуемые действия, обеспечивающие возможность восстановления базы данных: создайте резервные копии базы данных, файла хронологии тома, файла конфигурации устройств и файла опций сервера.

Если вы используете службу управления клиентами, убедитесь, что вы обновили ее до той же версии, к которой относится сервер IBM Spectrum Protect.

Убедитесь, что вы сохранили установочный носитель базового выпуска установленного сервера. Если вы устанавливали IBM Spectrum Protect из скачанного пакета, то убедитесь, что доступны скачанные файлы. Если обновление завершится неудачно и модуль лицензий сервера будет при этом деинсталлирован, то носитель установки базового выпуска сервера понадобится, чтобы переустановить лицензию.

Посетите страницу IBM Support Portal и найдите там следующую информацию:

- Список последних исправлений и их скачивание. Щелкните по **Downloads** (Материалы для скачивания) и примените все соответствующие исправления.
- Подробности получения базового пакета лицензий. Найдите **Downloads > Passport Advantage** (Материалы для скачивания - Passport Advantage).
- Поддерживаемые платформы и системные требования. Укажите для поиска: **поддерживаемые операционные системы IBM Spectrum Protect**.

Обязательно обновите сервер, прежде чем обновлять клиенты резервного копирования и архивирования. Если не обновить сначала сервер, связь между серевром и клиентами может прерваться.

Внимание: Не изменяйте программу Db2, устанавливаемую вместе с пакетами установки и пакетами исправлений IBM Spectrum Protect. Не устанавливайте другую версию, выпуск или пакет исправлений и не производите обновление до другой версии, выпуска или пакета исправлений программы Db2, так как это может привести к повреждению базы данных.

Процедура

Чтобы установить пакет исправлений или промежуточное исправление, сделайте следующее:

1. Создайте резервную копию базы данных. Рекомендуется способ использовать резервное копирование в режиме снимка. Резервное копирование в режима снимка - это полное резервное копирование базы данных, не прерывающее никаких плановых операций резервного копирования базы данных. Например, введите следующую команду управления IBM Spectrum Protect:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```

2. Создайте резервную копию информации о конфигурации устройств. Введите следующую команду управления IBM Spectrum Protect:

   ```
   backup devconfig filenames=имя_файла
   ```

   где *имя_файла* - это имя файла, в котором будет храниться информация о конфигурации устройств.

3. Сохраните файл хронологии томов в другом положении или переименуйте этот файл. Введите следующую команду управления IBM Spectrum Protect:

   ```
   backup volhistory filenames=имя_файла
   ```

   где *имя_файла* - это имя файла, в котором будет храниться информация хронологии томов.

4. Сохраните копию файла серверных опций, называемого, как правило, `dsmserv.opt`. Этот файл расположен в каталоге экземпляра сервера.

5. Прежде чем устанавливать пакет исправлений или промежуточное исправление, остановите сервер.

   Используйте команду **HALT**.

6. Убедитесь, что в каталоге установки доступно дополнительное пространство.

   Установка этого пакета Fix Pack может потребовать дополнительного временного дискового пространства в каталоге установки сервера. Объем дополнительного дискового пространства может быть таким же, как требуется для установки новой базы данных как части установки IBM Spectrum Protect. Мастер по установке IBM Spectrum Protect показывает объем пространства, требуемого для установки пакета Fix Pack, и доступный объем пространства. Если требуемый объем пространства превышает доступный, установка прекращается. Если установка остановилась, добавьте требуемое дисковое пространство к файловой системе и перезапустите установку.

7. Войдите в систему от имени пользователя root.

8. Получите файл пакета исправлений или промежуточного исправления, который вы хотите установить, со страниц IBM Support Portal, Passport Advantage или Fix Central.

9. Перейдите в каталог, куда вы поместили выполняемый файл, и сделайте следующее.

   Совет: Файлы извлекаются в текущий каталог. Убедитесь, что исполняемый файл находится в каталоге, куда будут извлекаться файлы.

   a. Измените разрешения на доступ к файлам, введя следующую команду:

      ```
      chmod a+x 8.x.x.x-IBM-SPSRV-платформа.bin
      ```

      где *платформа* - это архитектура, в которой устанавливается IBM Spectrum Protect.

   b. Чтобы извлечь файлы установки, введите следующую команду:

      ```
      ./8.x.x.x-IBM-SPSRV-платформа.bin
      ```

10. Выберите один из следующих способов установки IBM Spectrum Protect.

    Важное замечание: После установки пакета исправлений не нужно снова выполнять все шаги по конфигурированию. Вы можете остановить программу после завершения установки, исправить все ошибки и перезапустить свои серверы.

    Установите программное обеспечение IBM Spectrum Protect одним из следующих способов:

Мастер установки
Выполните инструкции для вашей операционной системы.

“Установка IBM Spectrum Protect при помощи мастера установки” на стр. 86

Совет: Запустив мастер, щелкните в окне **IBM Installation Manager** по значку **Обновить**; не щелкайте по значкам **Установить** и **Изменить**.

Командная строка в режиме консоли
Выполните инструкции для вашей операционной системы.

“Установка IBM Spectrum Protect в режиме консоли” на стр. 87

Совет: Если в вашей системе используется несколько экземпляров сервера, запустите мастер установки только один раз. Мастер по установке обновит все экземпляры сервера.

Результаты

Исправьте ошибки, обнаруженные в процессе установки.

Если вы установили сервер с использованием мастера установки, то вы можете посмотреть журналы установки при помощи инструмента IBM Installation Manager. Щелкните по **Файл** > **Просмотреть журнал**. Чтобы собрать файлы журналов, щелкните в IBM Installation Manager по **Справка** > **Экспорт данных для анализа ошибок**.

Если вы установили сервер в режиме консоли или в режиме без вывода сообщений, то вы можете просмотреть журналы ошибок в каталоге журнала IBM Installation Manager, например:

```
/var/ibm/InstallationManager/logs
```

Глава 5. Обновление до V8.1

Чтобы воспользоваться преимуществами новых функций и обновлений продукта, обновите сервер IBM Spectrum Protect.

Прежде чем начать

Ознакомьтесь с информацией о планировании обновлений защиты в разделе “Что следует знать о защите перед установкой или обновлением сервера” на стр. 3.

Об этой задаче

Чтобы обновить сервер в той же операционной системе, смотрите инструкции по обновлению. Инструкции по перенастройке сервера в другую операционную систему смотрите в документе Процесс перенастройки и обновления IBM Spectrum Protect - Часто задаваемые вопросы.

Таблица 21. Инструкции по обновлению

Для обновления от версии	До версии	Смотрите следующую информацию
V8.1	V8.1 с пакетом исправлений V8.1 или промежуточным исправлением	Глава 4, “Установка пакета исправлений сервера IBM Spectrum Protect”, на стр. 115
V7.1	V8.1	“Установка сервера и проверка обновления” на стр. 122
V7.1	V8.1 с пакетом исправлений V8.1 или промежуточным исправлением	Глава 4, “Установка пакета исправлений сервера IBM Spectrum Protect”, на стр. 115
V5.5, V6.2 или V6.3	V8.1	IBM Spectrum Protect Процесс обновления и перенастройки - Часто задаваемые вопросы

Обновление версии 7 до версии 8.1 занимает примерно 20-50 минут. Результаты в вашей среде могут отличаться от результатов, полученных в лабораториях.

Информацию об обновлении в кластерной среде смотрите в разделе “Обновление сервера в кластерной среде” на стр. 125.

Чтобы вернуться к прежней версии сервера после обновления или перенастройки, вам потребуется полная резервная копия базы данных и программа установки для исходной версии сервера. У вас также должны быть следующие важнейшие файлы конфигурации:

- Файл хронологии тома
- Файл конфигурации устройств
- Файл серверных опций

Информация, связанная с данной

Процесс обновления и перенастройки IBM Spectrum Protect - Часто задаваемые вопросы

Обновление до V8.1

Сервер можно обновить непосредственно с V7.1 до V8.1. Деинсталировать V7.1 не нужно.

Прежде чем начать

Убедитесь, что вы сохранили носитель установки базового выпуска сервера, который вы обновляете. Если вы устанавливали компоненты сервера с DVD-диска, то убедитесь, что этот DVD-диск доступен. Если вы устанавливали компоненты сервера из скачанного пакета, то убедитесь, что доступны скачанные файлы. Если обновление завершится неудачно и модуль лицензий сервера будет при этом деинсталлирован, то носитель установки базового выпуска сервера понадобится, чтобы переустановить лицензию.

Совет: Для V8.1 и новее DVD-диски больше не поставляются.

Процедура

Чтобы обновить сервер до V8.1, выполните следующие задачи:

1. “Планирование обновления” на стр. 120
2. “Подготовка системы” на стр. 120
3. “Установка сервера и проверка обновления” на стр. 122

Планирование обновления

Перед обновлением сервера с V7.1 до V8.1 необходимо ознакомиться с соответствующей информацией о планировании, например, с требованиями к системе и замечаниями по выпуску. Затем, чтобы свести к минимуму влияние обновления на производственный процесс, выберите для обновления подходящие дату и время.

Об этой задаче

В лабораторных тестах процесс обновления сервера V7.1 до V8.1 занимал от 14 до 45 минут. Ваши результаты могут отличаться, в зависимости от вашей аппаратной и программной среды и от размера базы данных сервера.

Процедура

1. Ознакомьтесь с аппаратными и программными требованиями:

   Требования к системе для систем Linux

   Информацию о последних изменениях требований к системе смотрите на сайте поддержки IBM Spectrum Protect в техническом замечании 1243309.
2. Особые инструкции или особую информацию для вашей операционной системы смотрите в замечаниях по выпуску (http://www.ibm.com/support/knowledgecenter/SSEQVQ_8.1.11/srv.common/r_relnotes_srv.html) и в файлах readme для компонентов сервера.
3. Ознакомьтесь с информацией о планировании обновлений защиты в разделе “Что следует знать о защите перед установкой или обновлением сервера” на стр. 3.
4. Чтобы свести к минимуму влияние обновления на производственный процесс, выберите для обновления подходящие дату и время. Время, которое требуется для обновления системы, зависит от размера базы данных и многих других факторов. При запуске процесса обновления клиенты не смогут соединиться с сервером, пока не будет установлена новая версия и не будут снова зарегистрированы все необходимые лицензии.
5. Если вы выполняете обновление сервера версии 7 до версии 8.1, убедитесь, что у вас есть системные ID и пароль для экземпляра IBM Db2 сервера IBM Spectrum Protect. Эти учетные данные необходимы для обновления системы.

Подготовка системы

Чтобы подготовить систему к обновлению с V7.1 до V8.1, нужно собрать информацию о каждом экземпляре IBM Db2. Затем создайте резервную копию базы данных сервера, сохраните ключевые файлы конфигурации, отмените сеансы и остановите сервер.

Процедура

1. Войдите в систему на компьютере, где установлен сервер.

   Проверьте, что вы вошли в систему под ID пользователя экземпляра.
2. Получите список экземпляров Db2. Например, введите следующую команду системы:

   ```
   /opt/tivoli/tsm/db2/instance/db2ilist
   ```

   Результат выполнения команды может выглядеть, как в следующем примере:

   ```
   tsminst1
   ```

   Убедитесь, что каждый экземпляр соответствует серверу, запущенному в этой системе.
3. Для каждого экземпляра Db2 запишите каталог базы данных по умолчанию, фактический каталог базы данных, имя базы данных, алиас базы данных и все переменные Db2, сконфигурированные для этого экземпляра. Сохраните запись, так как она может понадобиться. Эти сведения нужны для восстановления базы данных V7.1.
4. Соединитесь с сервером, указав ID пользователя-администратора.
5. Создайте резервную копию базы данных при помощи команды **BACKUP DB**.

   Рекомендуется использовать резервное копирование в режиме снимка, которое создает полную резервную копию базы данных без прерывания запланированного резервного копирования.

   Например, можно создать резервную копию снимка, введя следующую команду администрирования:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```
6. Создайте в другом каталоге резервную копию информации о конфигурации устройств при помощи следующей команды администрирования:

   ```
   backup devconfig filenames=имя_файла
   ```

   где *имя_файла* - это имя файла, в котором будет храниться информация о конфигурации устройств.

   Совет: Этот файл потребуется, если вы решите восстановить базу данных V7.1.
7. Скопируйте файл хронологии томов в другой каталог. Введите следующую команду администрирования:

   ```
   backup volhistory filenames=имя_файла
   ```

   где *имя_файла* - это имя файла, в котором будет храниться информация хронологии томов.

   Совет: Этот файл потребуется, если вы решите восстановить базу данных V7.1.
8. Сохраните копию файла серверных опций, называемого, как правило, `dsmserv.opt`. Этот файл расположен в каталоге экземпляра сервера.
9. Запретите операции на сервере, отключив новые сеансы. Введите следующие административные команды:

   ```
   disable sessions client
   disable sessions server
   ```
10. Проверьте, существуют ли какие-либо сеансы, и сообщите пользователям, что сервер будет остановлен. Чтобы проверить наличие существующих сеансов, введите команду администрирования:

    ```
    query session
    ```
11. Отмените сеансы, введя следующую команду администрирования:

```
cancel session all
```

Эта команда отменяет все сеансы, кроме вашего текущего сеанса.

12. Остановите сервер, введя следующую команду администрирования:

```
halt
```

13. Убедитесь, что сервер завершил работу и никакие процессы не выполняются.

    Введите следующую команду:

```
ps -ef | grep dsmserv
```

14. В каталоге экземпляра сервера вашей установки найдите файл NODELOCK и переместите его в другой каталог, где вы сохраняете файлы конфигурации.

    Файл NODELOCK содержит сведения об использованных лицензиях для вашей установки. Эта информация о лицензиях заменяется при выполнении обновления.

Установка сервера и проверка обновления

Чтобы завершить процесс обновления сервера до V8.1, необходимо установить сервер V8.1. Затем убедитесь, что обновление прошло успешно, запустив экземпляр сервера.

Прежде чем начать

Вы должны быть зарегистрированы в системе под ID пользователя root.

Пакет установки можно получить с сайта скачивания IBM.

Задайте предел максимального размера файла для системного пользователя, чтобы убедиться, что файлы можно успешно скачать.

1. Чтобы запросить значение для максимального размера файла, введите следующую команду:

```
ulimit -Hf
```

2. Если предельный максимальный размер файла для системного пользователя не задан как неограниченный, измените параметр на неограниченный, выполнив инструкции в документации для вашей операционной системы.

Об этой задаче

При помощи программы установки IBM Spectrum Protect можно установить следующие компоненты:

- Сервер

  Совет: База данных (IBM Db2), Global Security Kit (GSKit) и IBM Java Runtime Environment (JRE) автоматически устанавливаются при выборе компонента сервера.
- Языки сервера
- Лицензия
- Устройства
- IBM Spectrum Protect for SAN
- Центр операций

Процедура

1. Скачайте соответствующий файл пакета с одного из следующих веб-сайтов:
   - Скачайте пакет сервера со страницы Passport Advantage или Fix Central.

- Самую последнюю информацию, обновления и исправления обслуживания смотрите в разделе IBM Support Portal.

2. Выполните следующие шаги:

   a. Убедитесь, что у вас будет достаточно места для хранения файлов установки, когда они будут извлечены из пакета продукта. Требования к пространству смотрите в документе по скачиванию для вашего продукта.

      - IBM Spectrum Protect technote 588021
      - IBM Spectrum Protect Extended Edition technote 588023
      - IBM Spectrum Protect for Data Retention technote 588025

   b. Скачайте файл пакета в каталог по вашему выбору. Имя каталога может содержать не более 128 символов. Убедитесь, что извлекаете файлы установки в пустой каталог. Не выполняйте извлечение в каталог с ранее извлеченными файлами или с какими-либо еще файлами.

      Кроме того, у вас должны быть разрешения на запуск выполняемых файлов для файла пакета.

   c. Если потребуется, введите следующую команду, чтобы изменить разрешения на доступ к файлам:

      ```
      chmod a+x имя_пакета.bin
      ```

      где *имя_пакета* выглядит как в следующем примере:

      ```
      8.1.x.000-IBM-SPSRV-Linuxs390x.bin
      8.1.x.000-IBM-SPSRV-Linuxx86_64.bin
      8.1.x.000-IBM-SPSRV-Linuxppc64le.bin
      ```

      В примерах *8.1.x.000* представляет уровень выпуска продукта.

   d. Извлеките файлы установки, введя следующую команду:

      ```
      ./имя_пакета.bin
      ```

      Это большой пакет. Поэтому извлечение файлов займет некоторое время.

3. Установите программное обеспечение IBM Spectrum Protect одним из следующих способов. Установите лицензию на IBM Spectrum Protect в процессе установки.

   Совет: Если в системе используется несколько экземпляров сервера, установите программу IBM Spectrum Protect только один раз, чтобы обновить все экземпляры сервера.

   Мастер установки

   Чтобы установить сервер при помощи графического мастера IBM Installation Manager, выполните инструкции из раздела “Установка IBM Spectrum Protect при помощи мастера установки” на стр. 86.

   Убедитесь, что система соответствует обязательным требованиям для использования мастера установки. Затем выполните процедуру установки. В окне **IBM Installation Manager** щелкните по значку **Обновить** или **Изменить**.

   Установка сервера с использованием режима консоли

   Чтобы установить сервер в режиме консоли, следуйте инструкциям в разделе “Установка IBM Spectrum Protect в режиме консоли” на стр. 87.

   Ознакомьтесь с информацией об установке сервера в режиме консоли и затем выполните процедуру установки.

Режим без вывода сообщений

Чтобы установить сервер в режиме без вывода сообщений, выполните инструкции из раздела “Установка IBM Spectrum Protect в режиме без вывода сообщений” на стр. 87.

Ознакомьтесь с информацией об установке сервера в режиме без вывода сообщений и затем выполните процедуру установки.

После установки программы переконфигурировать систему не нужно.

4. Исправьте ошибки, обнаруженные в процессе установки.

   Если вы установили сервер с использованием мастера установки, то вы можете посмотреть журналы установки при помощи инструмента IBM Installation Manager. Щелкните по **Файл** > **Просмотреть журнал**. Чтобы собрать файлы журналов, щелкните в IBM Installation Manager по **Справка** > **Экспорт данных для анализа ошибок**.

   Если вы установили сервер в режиме консоли или в режиме без вывода сообщений, то вы можете просмотреть журналы ошибок в каталоге журнала IBM Installation Manager, например:

   ```
   /var/ibm/InstallationManager/logs
   ```

5. Перейдите в раздел IBM Support Portal, чтобы получить исправления. Щелкните по **Fixes, updates, and drivers** (Исправления, обновления и драйверы) и примените все необходимые исправления.
6. Проверьте, успешно ли выполнено обновление:
   a) Запустите экземпляр сервера.
   b) Следите за сообщениями, которые сервер генерирует при запуске. Следите за сообщениями об ошибках и предупреждениями и разрешите соответствующие проблемы.
   c) Проверьте, можете ли вы соединиться с сервером с помощью клиента администрирования. Для запуска сеанса клиента администрирования введите следующую команду администрирования IBM Spectrum Protect:

      ```
      dsmadmc
      ```

   d) Запустите команды **QUERY** для получения информации об обновленной системе. Например, чтобы получить объединенную информацию о системе, введите следующую команду администрирования IBM Spectrum Protect:

      ```
      query system
      ```

      Для получения информации о базе данных введите следующую команду администрирования IBM Spectrum Protect:

      ```
      query db format=detailed
      ```

7. Зарегистрируйте лицензии для установленных в вашей системе компонентов сервера IBM Spectrum Protect, введя команду **REGISTER LICENSE**:

   ```
   register license file=каталог_установки/server/bin/имя_компонента.lic
   ```

   где *каталог_установки* указывает каталог, в который вы установили компонент, а *имя_компонента* указывает аббревиатуру для этого компонента.

   Например, если вы установили сервер в каталоге по умолчанию `/opt/tivoli/tsm`, введите следующую команду, чтобы зарегистрировать лицензию:

   ```
   register license file=/opt/tivoli/tsm/server/bin/tsmbasic.lic
   ```

   Например, если вы установили IBM Spectrum Protect Extended Edition в каталог `/opt/tivoli/tsm`, введите следующую команду:

   ```
   register license file=/opt/tivoli/tsm/server/bin/tsmee.lic
   ```

Например, если вы установили IBM Spectrum Protect for Data Retention в каталог `/opt/tivoli/tsm`, введите следующую команду:

```
register license file=/opt/tivoli/tsm/server/bin/dataret.lic
```

Ограничение:

Вы не можете использовать сервер IBM Spectrum Protect для регистрации лицензий на следующие продукты:

- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for ERP
- IBM Spectrum Protect for Space Management

Команда **REGISTER LICENSE** не применяется к этим лицензиям. Лицензирование этих продуктов выполняется клиентами IBM Spectrum Protect.

8. Подготовьте сервер к автоматическим и ручным операциям резервного копирования базы данных.

   Инструкции смотрите в разделе “Подготовка сервера к операциям резервного копирования базы данных ” на стр. 111.
9. Необязательно: Для установки дополнительного пакета поддержки национального языка используйте функцию изменения IBM Installation Manager.
10. Необязательно: Для обновления языкового пакета до более новой версии используйте функцию обновления IBM Installation Manager.
11. Чтобы упростить устранение неполадок на случай возникновения в будущем каких-либо проблем, убедитесь, что для дампа ядра выделено достаточно пространства. Дополнительную информацию смотрите в техническом замечании 6357399.

Дальнейшие действия

Пароли можно аутентифицировать с помощью сервера каталогов LDAP или сервера IBM Spectrum Protect. Пароли, которые аутентифицированы с помощью сервера каталогов LDAP, могут обеспечить расширенную защиту системы.

Обновление сервера в кластерной среде

Чтобы обновить сервер в кластерной среде, нужно выполнить задачи подготовки и установки. Эти процедуры зависят от операционной системы и выпуска.

Процедура

Выполните процедуру для используемой операционной системы, исходной версии и версии назначения:

Таблица 22. Процедуры по обновлению сервера в кластерной среде в операционной системе Linux

Исходный выпуск	Выпуск назначения	Процедура
Версия 6.3 или более поздняя	V8.1	Обновление сервера, сконфигурированного с System Automation for Multiplatforms

Обновление IBM Spectrum Protect в кластерной среде

Для использования новых функций IBM Spectrum Protect можно обновить сервер IBM Spectrum Protect, установленный в Linux в кластерной среде.

Процедура

Чтобы выполнить обновление, следуйте инструкциям в разделе Конфигурирование среды Linux для кластеризации.

Глава 6. Справочная информация: Команды IBM Db2 для баз данных сервера IBM Spectrum Protect

Используйте этот список как справочник, если служба поддержки IBM предложит вам ввести команды Db2.

Назначение

Иногда после использования мастеров по установке и конфигурированию IBM Spectrum Protect вам потребуется ввести команды Db2. Ограниченный набор команд Db2, которые вы можете использовать (в частности, по указанию службы поддержки), представлен в таблице.

Это не исчерпывающий список, он представлен только в виде дополнительного материала. Не предполагается, что администратор IBM Spectrum Protect будет ежедневно или вообще регулярно использовать эти команды. Приведены примеры использования некоторых команд. Подробности выходной информации не представлены.

Полное объяснение описанных здесь команд и их синтаксиса смотрите в документации по продукту Db2.

Таблица 23. Команды DB2

Команда	Описание	Пример
db2icrt	Создает экземпляры Db2 в домашнем каталоге владельца экземпляра. **Совет:** Мастер по конфигурированию IBM Spectrum Protect создает экземпляр, используемый сервером и базой данных. После того, как сервер установлен и сконфигурирован с помощью мастера по конфигурированию, команда **db2icrt** обычно не используется. Эта утилита находится в каталоге `DB2DIR/instance`, где `DB2DIR` представляет собой положение установки текущей версии системы баз данных Db2.	Создайте экземпляр IBM Spectrum Protect вручную.Введите команду в одной строке: `/opt/tivoli/tsm/db2/instance/db2icrt -a server -u` *`имя_экземпляра имя_экземпляра`*
db2set	Выводит переменные Db2.	Вывести список переменных Db2: `db2set`
CATALOG DATABASE	Сохраняет информацию о положении базы данных в системном каталоге баз данных. База данных может находиться или на локальной рабочей станции, или на удаленном сервере разделов базы данных. Мастер по конфигурированию серверов учитывает все каталоги, которые нужны для использования базы данных сервера. После того, как сервер сконфигурирован и запущен, вручную запустите эту команду, только если что-то в среде изменяется или повреждено.	Каталогизируйте базу данных: `db2 catalog database tsmdb1`
CONNECT TO DATABASE	Соединяется с заданной базой данных для использования интерфейса командной строки (command-line interface, CLI).	Соединитесь с базой данных IBM Spectrum Protect в интерфейсе командной строки Db2: `db2 connect to tsmdb1`

Таблица 23. Команды DB2 (продолжение)

Команда	Описание	Пример

GET DATABASE CONFIGURATION	Возвращает значения индивидуальных записей в файле конфигурации конкретной базы данных.
	
	Важное замечание: Эти параметры и команды задаются и управляются непосредственно Db2. Они перечислены здесь в информационных целях и служат для просмотра существующих параметров. Изменение этих параметров может быть рекомендовано службой поддержки IBM или в служебных бюллетенях, таких как APAR или документы Технического руководства (technotes). Не изменяйте эти параметры вручную. Изменяйте их только по указанию службы технической поддержки IBM и только с использованием команд или процедур сервера IBM Spectrum Protect.
		Показать информацию конфигурации для алиаса базы данных:
		
		`db2 get db cfg for tsmdb1`
		
		Получить информацию для проверки параметров конфигурации базы данных, режима журналов и техобслуживания.
		
		`db2 get db config for tsmdb1 show detail`

GET DATABASE MANAGER CONFIGURATION	Возвращает значения индивидуальных записей в файле конфигурации конкретной базы данных. **Важное замечание:** Эти параметры и команды задаются и управляются непосредственно Db2. Они перечислены здесь в информационных целях и служат для просмотра существующих параметров. Изменение этих параметров может быть рекомендовано службой поддержки IBM или в служебных бюллетенях, таких как APAR или документы Технического руководства (technotes). Не изменяйте эти параметры вручную. Изменяйте их только по указанию службы технической поддержки IBM и только с использованием команд или процедур сервера IBM Spectrum Protect.	Получить информацию конфигурации для менеджера баз данных: `db2 get dbm cfg`
GET HEALTH SNAPSHOT	Получает информацию о состоянии работоспособности для менеджера баз данных и его баз данных. Возвращаемая информация представляет снимок состояния работоспособности на момент ввода команды. IBM Spectrum Protect отслеживает состояние базы данных при помощи снимка работоспособности и других механизмов, представленных Db2. Может так случиться, что снимок работоспособности или другая документация указывает на то, что элемент или ресурс базы данных может находиться в состоянии оповещения. Это означает, что нужно принять меры для исправления ситуации. IBM Spectrum Protect отслеживает условия и отвечает соответствующим образом. Обрабатываются не все выявленные оповещения Db2.	Получить отчет об индикаторах отслеживания работоспособности Db2: `db2 get health snapshot for database on tsmdb1`

Таблица 23. Команды DB2 (продолжение)

Команда	Описание	Пример

GRANT (Полномочия базы данных)	Предоставляет полномочия, применимые ко всей базе данных, в отличие от полномочий, применимых к конкретным объектам в базе данных.	Предоставить доступ для ID пользователя itmuser:
		`db2 GRANT CONNECT ON DATABASE TO USER itmuser`
		`db2 GRANT CREATETAB ON DATABASE TO USER itmuser`

RUNSTATS	Изменяет статистику, относящуюся к характеристикам таблицы и связанных индексов, или статистические производные таблицы. Эти характеристики включают в себя количество записей, количество страниц и среднюю длину записи. Запустите эту утилиту, чтобы увидеть таблицу после ее изменения или реорганизации. Производная таблица должна быть включена для оптимизации, чтобы ее можно было использовать для оптимизации запросов. Включенная для оптимизации производная таблица называется статистической производной таблицей. Используйте оператор Db2 **ALTER VIEW** , чтобы включить производную таблицу для оптимизации. Запустите утилиту **RUNSTATS**, когда изменения в рассматриваемых таблицах существенно влияют на возвращаемые в производной таблице строки. **Совет:** Сервер конфигурирует Db2 для запуска при необходимости команды **RUNSTATS**.	Изменить статистику для одной таблицы. `db2 runstats on table SCHEMA_NAME.TABLE_NAME with distribution and sampled detailed indexes all`
SET SCHEMA	Изменяет значение специального регистра **CURRENT SCHEMA**, подготавливаясь к вводу команд SQL непосредственно через интерфейс командной строки Db2. **Совет:** Специальный регистр - это область хранения, определенная для процесса применения менеджером баз данных. Он используется для хранения информации, на которую могут ссылаться операторы SQL.	Задать схему для IBM Spectrum Protect: `db2 set schema tsmdb1`
START DATABASE MANAGER	Запускает фоновые процессы текущего экземпляра менеджера баз данных. Сервер запускает и останавливает экземпляр и базу данных при всех запусках и остановках сервера. **Важное замечание:** Разрешить серверу управлять запуском и остановкой экземпляра и базы данных, если иное не указано службой поддержки IBM.	Запустить менеджер баз данных: `db2start`

Таблица 23. Команды DB2 (продолжение)

Команда	Описание	Пример
STOP DATABASE MANAGER	Останавливает текущий экземпляр менеджера баз данных. Менеджер баз данных остается активным, пока он не остановлен явным образом. Эта команда не останавливает экземпляр менеджера баз данных, если какие-либо приложения соединены с базами данных. Если соединений с базой данных нет, но есть подключения экземпляра, эти подключения экземпляра первыми принудительно прерываются данной командой. Затем она останавливает менеджер баз данных. Перед остановкой менеджера баз данных эта команда деактивирует также все невыполненные обращения к базе данных. Для клиента эта команда недопустима. Сервер запускает и останавливает экземпляр и базу данных при всех запусках и остановках сервера. **Важное замечание:** Разрешить серверу управлять запуском и остановкой экземпляра и базы данных, если иное не указано службой поддержки IBM.	Остановить менеджер баз данных: `db2 stop dbm`

Глава 7. Деинсталляция IBM Spectrum Protect

Ниже описаны процедуры по деинсталляции IBM Spectrum Protect. Прежде чем удалять IBM Spectrum Protect, убедитесь, что вы не потеряете ваши резервные копии и архивные данные.

Прежде чем начать

Прежде чем деинсталлировать IBM Spectrum Protect, выполните следующие шаги:

- Выполните полное резервное копирование базы данных.
- Сохраните копию хронологии томов и файлов конфигурации устройств.
- Поместите полученные тома в надежное место.

Об этой задаче

IBM Spectrum Protect можно деинсталлировать любым из следующих способов: графический мастер, командная строка в режиме консоли или режим без вывода сообщений.

Дальнейшие действия

Повторно установите компоненты IBM Spectrum Protect.

Деинсталляция IBM Spectrum Protect при помощи графического мастера

IBM Spectrum Protect можно деинсталлировать при помощи мастера установки IBM Installation Manager.

Процедура

1. Запустите Installation Manager.

   В каталоге, в котором установлен Installation Manager, перейдите в подкаталог `eclipse` (например, `/opt/IBM/InstallationManager/eclipse`) и введите следующую команду:

   ```
   ./IBMIM
   ```

2. Щелкните по **Деинсталлировать**.
3. Выберите **Сервер IBM Spectrum Protect** и нажмите кнопку **Далее**.
4. Щелкните по **Деинсталлировать**.
5. Щелкните по **Готово**.

Деинсталляция IBM Spectrum Protect в режиме консоли

Чтобы деинсталлировать IBM Spectrum Protect из командной строки, запустите программу деинсталляции IBM Installation Manager из командной строки, указав параметр для режима консоли.

Процедура

1. В каталоге, в котором установлен IBM Installation Manager, перейдите в следующий подкаталог:

   `eclipse/tools`

   Например:

   `/opt/IBM/InstallationManager/eclipse/tools`

2. В каталоге `tools` введите следующую команду:

   ```
   ./imcl -c
   ```
3. Для деинсталляции введите 5.
4. Выберите деинсталляцию в группе пакетов IBM Spectrum Protect.
5. Введите N (Next - Далее).
6. Выберите деинсталляцию пакета сервера IBM Spectrum Protect.
7. Введите N (Next - Далее).
8. Введите U (Uninstall - Деинсталляция).
9. Введите F (Finish - Готово).

Деинсталляция IBM Spectrum Protect в режиме без вывода сообщений

Чтобы деинсталлировать IBM Spectrum Protect в режиме без вывода сообщений, запустите программу деинсталляции IBM Installation Manager из командной строки, указав параметры для режима без вывода сообщений.

Прежде чем начать

Вы можете использовать файл ответов, чтобы задать входные данные для деинсталляции компонентов сервера IBM Spectrum Protect в режиме без вывода сообщений. IBM Spectrum Protect содержит пример файла ответов, `uninstall_response_sample.xml`, в каталоге `input` в том месте, куда был распакован пакет установки. Этот файл содержит значения по умолчанию, которые помогут вам избежать ненужных предупреждений.

Если вы хотите деинсталлировать все компоненты IBM Spectrum Protect, оставьте заданное значение `modify="false"` для каждого компонента в файле ответов. Если вы не хотите деинсталлировать компонент, задайте значение `modify="true"`.

Если вы хотите настроить файл ответов, вы можете изменить опции, содержащиеся в файле. Информацию о файлах ответов смотрите в разделе Файлы ответов.

Процедура

1. В каталоге, в котором установлен IBM Installation Manager, перейдите в следующий подкаталог:

   ```
   eclipse/tools
   ```

   Например:

   ```
   /opt/IBM/InstallationManager/eclipse/tools
   ```
2. В каталоге `tools` введите следующую команду, где *файл_ответов* - это полное имя файла ответов:

   ```
   ./imcl -input файл_ответов -silent
   ```

   Пример команды:

   ```
   ./imcl -input /tmp/input/uninstall_response.xml -silent
   ```

Деинсталляция и переустановка IBM Spectrum Protect

Если вы собираетесь переустановить IBM Spectrum Protect вручную, а не пользоваться мастером, вы должны будете выполнить ряд шагов, чтобы сохранить имена экземпляров сервера и каталогов баз данных. При деинсталляции все имеющиеся у вас экземпляры сервера удаляются, но каталоги для этих экземпляров остаются.

Об этой задаче

Чтобы вручную деинсталлировать и переустановить IBM Spectrum Protect, выполните следующие шаги:

1. Прежде чем приступать к деинсталляции, создайте список текущих экземпляров сервера. Выполните команду:

   ```
   /opt/tivoli/tsm/db2/instance/db2ilist
   ```

2. Введите для каждого экземпляра сервера следующую команду:

   ```
   db2 attach to имя_экземпляра
   db2 get dbm cfg show detail
   db2 detach
   ```

   Запишите путь базы данных для каждого экземпляра.

3. Деинсталлируйте IBM Spectrum Protect.
4. При деинсталляции любой поддерживаемой версии IBM Spectrum Protect, включая пакет исправлений, создается файл экземпляра. Файл экземпляра создается для того, чтобы помочь вам переустановить IBM Spectrum Protect. Проверьте этот файл и используйте эту информацию, когда вас попросят ввести идентификационные данные экземпляра при переустановке. При установке в режиме без вывода сообщений вы предоставляете эти идентификационные данные при помощи переменной `INSTANCE_CRED`.

   Положение файла экземпляра:

   `/etc/tivoli/tsm/instanceList.obj`

5. Переустановите IBM Spectrum Protect.

   Если файл `instanceList.obj` не существует, вы должны заново создать экземпляры сервера, используя следующие шаги:

   a. Заново создайте экземпляры сервера.

      Совет: Мастер установки сконфигурирует экземпляры сервера, но вы должны убедиться, что они существуют. Если они не существуют, вы должны будете сконфигурировать их вручную.

   b. Каталогизируйте базу данных. Поочередно войдите в систему от имени пользователя экземпляра для каждого экземпляра сервера и введите следующие команды:

      ```
      db2 catalog database tsmdb1
      db2 attach to имя_экземпляра
      db2 update dbm cfg using dftdbpath каталог_экземпляра
      db2 detach
      ```

   c. Убедитесь, что экземпляр сервера создан успешно.Введите команду:

      ```
      /opt/tivoli/tsm/db2/instance/db2ilist
      ```

   d. Убедитесь, что IBM Spectrum Protect распознает экземпляры сервера, вызвав спи сок ваших каталогов. Вы увидите ваш домашний каталог (если вы его не изменили). Если вы использовали мастер конфигурирования, ваш каталог экземпляра не появится. Введите команду:

      ```
      db2 list database directory
      ```

      Если вы увидите в списке TSMDB1, вы можете запустить сервер.

Деинсталляция IBM Installation Manager

Можно деинсталлировать IBM Installation Manager, если у вас больше нет продуктов, установленных IBM Installation Manager.

Прежде чем начать

Перед удалением IBM Installation Manager, необходимо убедиться, что все пакеты, установленные IBM Installation Manager, удалены. Закройте IBM Installation Manager перед запуском деинсталляции.

Для просмотра установленных пакетов введите следующую команду в командной строке:

```
cd /opt/IBM/InstallationManager/eclipse/tools
./imcl listInstalledPackages
```

Процедура

Чтобы деинсталлировать IBM Installation Manager, сделайте следующее:

- 1. Откройте командную строку и перейдите в каталог `/var/ibm/InstallationManager/uninstall`.
  2. Введите следующую команду:

     ```
     ./uninstall
     ```

     Ограничение: Вы должны войти в систему от имени ID пользователя `root`.

Часть 2. Установка и обновление Центра операций

Центр операций IBM Spectrum Protect - это веб-интерфейс для управления средой хранения.

Прежде чем начать

Прежде чем приступить к установке и конфигурированию Центра операций, просмотрите следующую информацию:

- Требования к системе для Центра операций
  - Требования к компьютеру Центра операций
  - Требования к хаб-серверу и подчиненному серверу
  - Требования к операционной системе
  - Требования к веб-браузеру
  - Требования к языку
  - Требования и ограничения для Службы управления клиентами IBM Spectrum Protect
- Требующиеся Центру операций ID администратора
- IBM Installation Manager
- Контрольный список установки
- Получение пакета установки Центр операций

Об этой задаче

В Таблица 24 на стр. 135 перечислены методы установки и деинсталляции Центра операций и указано, где можно найти соответствующие инструкции.

Информацию об обновлении Центра операций смотрите в разделе Обновление Центр операций.

Таблица 24. Методы установки и деинсталляции Центра операций.

Method	**Инструкции**
Мастер графики	• Установка Центра операций при помощи графического мастера Центра операций • Деинсталляция Центра операций при помощи графического мастера Центра операций
Режим консоли	• Установка Центра операций в режиме консоли • Деинсталляция Центра операций в режиме консоли
Режим без вывода сообщений	• Установка Центра операций в режиме без вывода сообщений • “Деинсталляция Центра операций в режиме без вывода сообщений” на стр. 210

Глава 8. Планирование установки Центра операций

Прежде чем приступать к установке Центра операций, нужно выяснить требования к системе, ID администраторов, которые требует Центр операций, и информацию, которую нужно предоставить программе установки.

Об этой задаче

Из Центра операций можно управлять следующими основными аспектами среды хранения:

- Серверы и клиенты IBM Spectrum Protect
- Службы, такие, как служба резервного копирования и восстановления, архивирования и получения данных, а также перенастройки и возврата данных
- Пулы хранения и устройства хранения

Центр операций содержит следующие компоненты:

Пользовательский интерфейс для нескольких серверов
С помощью Центра операций можно управлять одним или несколькими серверами IBM Spectrum Protect.

В среде с несколькими серверами можно задать один сервер в качестве *хаб-сервера*, а остальные - в качестве *подчиненных серверов*. Хаб-сервер может получать оповещения и информацию о состоянии от подчиненных серверов и выдавать эту информацию в консолидированном представлении в Центре операций.

Мониторинг оповещений

Оповещение - это уведомление о проблеме на сервере; оповещение инициализируется сообщением сервера. Вы можете указать, какие сообщения сервера инициализируют оповещения, и в Центре операций или в электронной почте только эти сообщения будут показаны как оповещения.

Мониторинг оповещений может помочь выявить и отследить ошибки на сервере.

Удобный интерфейс командной строки
Центр операций содержит интерфейс командной строки для поддержки расширенных функций и конфигурирования.

Требования к системе для Центра операций

Прежде чем устанавливать Центр операций, убедитесь, что ваша система соответствует минимальным требованиям.

Воспользуйтесь страницей Калькулятор требований к системе для Центра операций, чтобы оценить требования к системе для работы Центра операций, а также хаб-сервера и подчиненных серверов, которые отслеживает Центр операций.

Требования, проверяемые во время установки

В таблице Таблица 25 на стр. 138 перечислены предварительные требования, проверяемые при установке, и указано, где найти дополнительную информацию об этих требованиях.

Таблица 25. Требования, проверяемые во время установки	
Требование	**Сведения**
Минимальные требования к памяти	“Требования к компьютеру для Центра операций” на стр. 138
Требования операционной системы	“Требования к операционной системе” на стр. 142
Имя хоста для компьютера, где будет установлен Центр операций	“Контрольный список установки” на стр. 146
Требования для каталога установки Центра операций	“Контрольный список установки” на стр. 146

Требования к компьютеру для Центра операций

Центр операций можно установить на компьютер, на котором работает сервер IBM Spectrum Protect, или на другой компьютер. Если вы устанавливаете Центр операций на тот же компьютер, что и сервер, этот компьютер должен соответствовать требованиям к системе и для Центра операций, и для сервера.

Требования к ресурсам

Для запуска Центра операций требуются следующие ресурсы:

- Одно процессорное ядро
- 4 ГБ памяти
- 1 ГБ пространства на диске

Хаб-серверу и подчиненным серверам, которые отслеживает Центр операций, нужны дополнительные ресурсы, как описано в разделе “Требования для хаб-сервера и подчиненных серверов” на стр. 138.

Требования для хаб-сервера и подчиненных серверов

Когда вы впервые открываете Центр операций, вы должны связать Центр операций с одним сервером IBM Spectrum Protect, заданным в качестве *хаб-сервера*. В среде с несколькими серверами можно подключить к хаб-серверу дополнительные серверы, которые называются *подчиненные серверы*.

Подчиненные серверы отправляют оповещения и информацию о состоянии хаб-серверу. Центр операций содержит консолидированное представление оповещений и информации о состоянии для хаб-сервера и всех подчиненных серверов.

Если Центром операций отслеживается только один сервер, то этот сервер все равно называется хаб-сервером, хотя к нему не подключен ни один подчиненный сервер.

В таблице Таблица 26 на стр. 139 указана версия сервера IBM Spectrum Protect, которая должна быть установлена на хаб-сервере и на каждом подчиненном сервере, которыми управляет Центр операций.

Таблица 26. Требования к версии сервера IBM Spectrum Protect для хаб-сервера и подчиненных серверов

Центр операций	Версия хаб-сервера	Версия на каждом подчиненном сервере
V8.1.12	V8.1.12	V8.1.10 или новее ========== или версия 7.1.10 или более поздние выпуски Версии 7 **Ограничения:** • Некоторые функции компонента Центр операций недоступны для серверов, использующих более раннюю версию, чем V8.1.12. • Подчиненный сервер не может использовать более новую версию, чем версия на хаб-сервере.

Информацию о требованиях совместимости хаб-сервера и подчиненных серверов для других версий Центра операций, смотрите в техническом замечании 496593.

Число подчиненных серверов, которое может поддерживать хаб-сервер

Число подчиненных серверов, которое может поддерживать хаб-сервер, зависит от конфигурации и от версии IBM Spectrum Protect на каждом подчиненном сервере. Однако можно принять в качестве общей рекомендации то, что один хаб-сервер в отдельной системе, например, виртуальная машина, может поддерживать десятки подчиненных серверов версии 7.1 или новее.

Советы по проектированию конфигурации хаб-сервера и подчиненных серверов

При проектировании конфигурации хаб-сервера и подчиненных серверов следует внимательно отнестись к требованиям ресурсов для мониторинга состояния. Кроме того, решите, как вы хотите группировать хаб-сервер и подчиненные серверы и хотите ли вы использовать несколько хаб-серверов.

Воспользуйтесь страницей Калькулятор требований к системе для Центра операций, чтобы оценить требования к системе для работы Центра операций, а также хаб-сервера и подчиненных серверов, которые отслеживает Центр операций.

Основные факторы, влияющие на производительность

На производительность Центра операций сильнее всего влияют следующие факторы:

- Процессор и память на компьютере, на котором установлен Центр операций
- Системные хаб-сервера и подчиненных серверов, включая дисковую систему, используемую для базы данных хаб-сервера.
- Число клиентских узлов и файловых пространств виртуальных машин, которые управляются хаб-сервером и подчиненными серверами
- Частота обновления данных в Центре операций

Как группировать хаб-сервер и подчиненные серверы

Группируйте хаб-сервер и подчиненные серверы по географическому положению. Например, управление серверами в пределах одного центра данных может предотвратить проблемы, связанные с брандмауэрами или недостаточной полосой пропускания между разными положениями. При необходимости серверы можно дополнительно подразделить в соответствии с одной или несколькими следующими характеристиками:

- Администратор, который управляет серверами.
- Объект организации, который финансирует серверы.
- Операционная система сервера
- Язык, на котором работают серверы

  Совет: Если хаб-сервер и подчиненные серверы работают на разных языках, то в Центре операций может выводится испорченный текст.

Как сгруппировать хаб-сервер и подчиненные серверы в конфигурации организации

В конфигурации организации сеть серверов IBM Spectrum Protect управляется как группа. Изменения, внесенные в *менеджере конфигурации*, можно автоматически распространить на один или несколько *управляемых серверов* в сети.

Обычно Центр операций регистрирует выделенный ID администратора на хаб-сервере и подчиненных серверах и управляет им. У этого *администратора мониторинга* всегда должен быть один и тот же пароль на всех серверах.

Если вы используете конфигурацию организации, то можно улучшить процесс синхронизации идентификационных данных администратора на подчиненных серверах. Чтобы повысить производительность и эффективность управления ID администратора, сделайте следующее:

1. Назначьте сервер менеджера конфигурации хаб-сервером Центра операций. Во время конфигурирования хаб-сервера регистрируется ID администратора мониторинга с именем IBM-OC-*имя_хаб-сервера*.
2. Добавьте на хаб-сервере ID администратора мониторинга в новый или в существующий профиль конфигурации организации. Введите команду NOTIFY SUBSCRIBERS, чтобы распространить профиль на управляемые серверы.
3. Добавьте один или несколько управляемых серверов в качестве подчиненных серверов Центра операций.

Центр операций обнаруживает эту конфигурацию и позволяет менеджеру конфигурации распространять ID администратора мониторинга на подчиненные серверы и изменять его.

Когда использовать несколько хаб-серверов

Если вы работаете больше, чем с 10-20 подчиненными серверами V6.3.4, или если из-за ограничений ресурсов требуется многораздельная среда, то вы можете сконфигурировать несколько хаб-серверов и подключить к каждому хаб-серверу поднабор подчиненных серверов.

Ограничения:

- Один сервер не может быть и хаб-сервером, и подчиненным сервером.
- Каждый подчиненный сервер может быть назначен только одному хаб-серверу.
- Для каждого хаб-сервера требуется отдельный экземпляр Центра операций, каждый из которых имеет свой веб-адрес.

Советы по выбору хаб-сервера

Для хаб-сервера нужно выбрать сервер с достаточными ресурсами, расположенный так, чтобы обеспечить минимальную задержку двусторонней сетевой связи.

Внимание: Не используйте один и тот же сервер в качестве хаб-сервера для нескольких Центров операций.

При выборе, какой сервер назначить хаб-сервером, руководствуйтесь следующими рекомендациями:

Выберите слабо нагруженный сервер

Выберите сервер с небольшой нагрузкой для операций (например, для резервного копирования клиентов и архивирования). Слабо нагруженный сервер также хорошо использовать в качестве системы хоста для Центра операций.

Убедитесь, что у сервера достаточно ресурсов для обслуживания и своей обычной рабочей нагрузки сервера, и оценочной нагрузки при работе в качестве хаб-сервера.

Расположите сервер так, чтобы обеспечить минимальную задержку двусторонней сетевой связи

Расположите хаб-сервер так, чтобы сетевое соединение между хаб-сервером и подчиненными серверами имело двустороннюю задержку не более 5 мс. Эта задержка обычно может быть достигнута, когда серверы находятся в одной и той же локальной сети (LAN).

Сети, которые плохо настроены, интенсивно используются другими приложениями или показывают двустороннюю задержку значительно больше 5 мс, могут ухудшить связь между хаб-сервером и подчиненными серверами. Например, двусторонняя задержка в 50 мс или выше может вызвать истечение срока ожидания связи, из-за чего подчиненные серверы будут отсоединяться от Центра операций или повторно соединяться с ним. Такие высокие задержки могут наблюдаться при связи через глобальные сети (wide area network, WAN) на большом расстоянии.

Если подчиненные серверы находятся на большом расстоянии от хаб-сервера, и в Центре операций наблюдаются частые разрывы соединений, можно увеличить значение опции **ADMINCOMMTIMEOUT** на каждом сервере, чтобы уменьшить частоту возникновения этой проблемы.

Убедитесь, что хаб-сервер соответствует требованиям к ресурсам для мониторинга состояния

Для мониторинга состояния требуются дополнительные ресурсы на каждом сервере, где он включен. Требуемые ресурсы зависят в первую очередь от числа клиентов, которые управляются хаб-сервером и подчиненными серверами. На хаб-сервере с подчиненным сервером V7.1 или новее используется меньше ресурсов, чем на хаб-сервере с подчиненным сервером V6.3.4.

Убедитесь, что хаб-сервер соответствует требованиям к ресурсам использования процессора, пространства для базы данных, пространства для архивных журналов и мощности операций ввода-вывода в секунду (I/O operations per second, IOPS).

Хаб-сервер с высокой мощностью IOPS может обрабатывать больший объем данных о состоянии, приходящих с подчиненных серверов. Эту мощность можно обеспечить при использовании следующих устройств хранения для базы данных хаб-сервера:

- Твердотельный накопитель (SSD) уровня предприятия
- Внешнее устройство дискового хранения SAN с несколькими томами или несколькими дисководами в каждом томе.

В среде, содержащей менее 1000 клиентов, задайте для базы данных хаб-сервера базовую емкость 1000 IOPS, если хаб-сервер управляет подчиненными серверами.

Определите, нужно ли в вашей среде несколько хаб-серверов

Если одним набором хаб-сервера и подчиненных серверов управляется более 10 000 - 20 000 клиентских узлов и файловых пространств виртуальных машин, требования к ресурсам могут превышать доступные ресурсы хаб-сервера, особенно если подчиненные серверы - это серверы V6.3.4. Возможно, следует назначить хаб-сервером второй сервер и переместить часть подчиненных серверов на новый хаб-сервер для балансировки нагрузки.

Требования к операционной системе

Центр операций доступен в системах AIX, Linux и Windows.

Центр операций может работать в следующих системах.

Поддержка Центр операций для систем AIX и Linux ограничена только версиями Big Endian, если не указано иное.

- Linux в системах x86_64:
  - Red Hat® Enterprise Linux 8.1 или новее
  - Red Hat Enterprise Linux 7.6 или новее
  - SUSE Linux Enterprise Server 15 с Service Pack 1 или новее
  - SUSE Linux Enterprise Server 12 с Service Pack 4 или новее
- Linux в системах System z (64-разрядная архитектура s390x):
  - Red Hat Enterprise Linux 8.1 или новее
  - Red Hat Enterprise Linux 7.6 или новее
  - SUSE Linux Enterprise Server 15 с Service Pack 1 или новее
  - SUSE Linux Enterprise Server 12 с Service Pack 4 или новее
- Linux в системах Power Systems (с прямым порядком байтов):
  - Red Hat Enterprise Linux 8.1 или новее
  - Red Hat Enterprise Linux 7.6 или новее с архитектурой PPC64LE
  - SUSE Linux Enterprise Server 15 с Service Pack 1 или новее
  - SUSE Linux Enterprise Server 12 с Service Pack 4 или новее

Самую последнюю информацию о требованиях смотрите в документе Требования к аппаратному и программному обеспечению.

Требования к веб-браузеру

Центр операций работает в браузерах Apple, Google, Microsoft и Mozilla.

Для оптимального просмотра Центра операций в браузере задайте в системе разрешение экрана, как минимум, 1024 X 768 пикселей.

Для оптимальной производительности используйте браузер с хорошей производительностью JavaScript и включите кэширование браузера.

Центр операций работает в следующих браузерах:

- Apple Safari на iPad

  Ограничение: Если Apple Safari работает в iOS 8.x или iOS 9.x, вы не сможете использовать самоподписанный сертификат для защищенных взаимодействий с центром операций, не произведя дополнительного конфигурирования сертификата. Используйте сертификат сертификатора (certificate authority, CA) или сконфигурируйте самоподписанный сертификат нужным образом. Инструкции смотрите в техническом примечании по адресу: http://www.ibm.com/support/docview.wss?uid=swg21963153.
- Google Chrome 54 или новее
- Microsoft Internet Explorer 11 или новее
- Mozilla Firefox ESR 45 или версии 48 либо новее

Связь между компонентом Центр операций и веб-браузером должна быть защищена с использованием протокола Transport Layer Security (TLS) 1.2. Веб-браузер должен поддерживать протокол TLS 1.2, и этот протокол должен быть включен. Если эти требования не выполняются, в веб-браузере появится ошибка SSL.

Самую последнюю информацию о требованиях смотрите в документе Требования к аппаратному и программному обеспечению.

Требования языка

По умолчанию Центр операций использует язык, заданный для веб-браузера. Однако процесс установки использует язык операционной системы. Убедитесь, что для веб-браузера и операционной системы задан нужный язык.

Таблица 27. Значения языков Центра операций, которые можно использовать в системах Linux

Язык	**Значение опции языка**
Китайский упрощенный	zh_CN
Китайский упрощенный (GBK)	zh_CN.gb18030
Китайский упрощенный (UTF-8)	zh_CN.utf8
Китайский традиционный (Big5)	Zh_TW
Китайский традиционный (euc_tw)	zh_TW
Китайский традиционный (UTF-8)	zh_TW.utf8
Английский, США	en_US
Английский (UTF-8)	en_US.utf8
Французский	fr_FR
Французский (UTF-8)	fr_FR.utf8
Немецкий	de_DE
Немецкий (UTF-8)	de_DE.utf8
Итальянский	it_IT
Итальянский (UTF-8)	it_IT.utf8
Японский (EUC)	ja_JP
Японский (UTF-8)	ja_JP.utf8
Корейский	ko_KR
Корейский (UTF-8)	ko_KR.utf8
Бразильский португальский	pt_BR
Бразильский португальский (UTF-8)	pt_BR.utf8
Русский	ru_RU
Русский (UTF-8)	ru_RU.utf8
Испанский	es_ES
Испанский (UTF-8)	es_ES.utf8

Требования и ограничения для службы управления клиентом

Службы управления клиентами IBM Spectrum Protect - это компонент, устанавливаемый на клиентах резервного копирования и архивирования для сбора диагностической информации (например, файлов журнала клиента). Перед установкой компонента служба управления клиентами в вашей системе нужно ознакомиться с требованиями и ограничениями.

В документации к службе управления клиентом *компьютер клиента* - это компьютер, на котором установлен клиент резервного копирования и архивирования.

Диагностическую информацию можно собрать только с клиентов Linux и Windows, но администраторы могут просматривать диагностическую информацию по компоненту Центр операций в операционных системах AIX, Linux или Windows.

Совет: Перед установкой служба управления клиентами убедитесь, что между клиентом резервного копирования-архивирования и сервером успешно установлено соединение. В файле склада доверенных сертификатов сервера, используемого клиентом, не будет сертификата Secure Sockets Layer (SSL) сервера, пока система клиента не соединится с сервером.

Требования для службы управления клиентом

Перед установкой службы управления клиентом убедитесь, что выполнены следующие требования:

- Для удаленного доступа к клиенту у администратора Центра операций должны быть системные полномочия или один из следующих уровней полномочий клиента:
  - Полномочия Политика
  - Полномочия владельца клиента
  - Полномочия доступа к клиентскому узлу
- Убедитесь, что компьютер клиента соответствует следующим требованиям:
  - Службу управления клиентом можно установить только на компьютерах клиента со следующими операционными системами Linux или Windows:
    - Linux x86 (64-разрядные), поддерживаемые для клиента резервного копирования и архивирования.
    - Windows (32- и 64-разрядные), поддерживаемые для клиента резервного копирования и архивирования.
  - Для передачи данных между компонентом служба управления клиентами и компонентом Центр операций должен быть установлен протокол Transport Layer Security (TLS) версии 1.2 или новее. Обеспечивается базовая аутентификация, и данные и информация аутентификации шифруются через канал Secure Sockets Layer (SSL). TLS и необходимые сертификаты SSL автоматически устанавливаются при установке компонента служба управления клиентами.

    Начиная с IBM Spectrum Protect версии 8.1.11, протокол TLS 1.3 включается по умолчанию для защиты соединений между серверами, клиентами и агентами хранения. Чтобы использовать TLS 1.3, обе стороны в сеансе связи должны использовать TLS 1.3. Если любая из сторон использует TLS 1.2, по умолчанию обе стороны используют TLS 1.2.
- На компьютерах клиента Linux для установки службы управления клиентом требуются полномочия пользователя root.
- Для компьютеров клиентов с несколькими клиентскими узлами (например, компьютеры клиентов Linux) убедитесь, что имя каждого узла уникально на компьютере клиента.

  Совет: После установки службы управления клиентом ее не нужно устанавливать повторно, так как служба может обнаруживать несколько файлов опций клиента.

Ограничения службы управления клиентом

Служба управления клиентом предоставляет базовые службы для сбора диагностической информации в клиентах резервного копирования и архивирования. Ниже перечислены ограничения для службы управления клиентом:

- Вы можете установить компонент служба управления клиентами только в системах с клиентами резервного копирования и архивирования, включая клиентов резервного копирования и архивирования, установленных на узлах перемещения данных для IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

- Установить компонент служба управления клиентами на других компонентах клиентов или в других продуктах IBM Spectrum Protect, у которых нет клиентов резервного копирования и архивирования, вы не можете.
- Если клиенты резервного копирования и архивирования защищены брандмауэром, убедитесь, что компонент Центр операций может соединиться с клиентами резервного копирования и архивирования через брандмауэр, используя порт, сконфигурированный для компонента служба управления клиентами. Порт по умолчанию - 9028, но его можно изменить.
- Служба управления клиентом сканирует все файлы журнала клиента, чтобы найти записи, созданные в течение предыдущих 72 часов.
- На странице **Диагностика** в Центре операций содержится основная диагностическая информация для клиентов резервного копирования и архивирования. Однако вам может понадобиться доступ к компьютеру клиента и дополнительная диагностическая информация для устранения некоторых проблем резервного копирования.
- Если общий размер файлов журнала ошибок клиента и файлов журнала расписания больше 500 МБ, то при отправке записей журнала в Центре операций могут возникнуть задержки. Для управления размером файлов журнала можно разрешить сокращение или перенос файлов журнала при помощи опций клиента **errorlogretention** или **errorlogmax**.
- Если вы используете одно и то же имя клиентского узла для соединения с несколькими серверами IBM Spectrum Protect, которые установлены на одном и том же сервере, вы можете посмотреть файлы журнала только для одного из клиентских узлов.

Чтобы узнать о возможных обновлениях, касающихся компонента служба управления клиентами, смотрите техническое замечание 534165.

Задачи, связанные с данной

“Сбор диагностической информации посредством службы управления клиентом Tivoli Storage Manager” на стр. 185
служба управления клиентами собирает диагностическую информацию о клиентах резервного копирования и архивирования и делает ее доступной для Центра операций для основных функций мониторинга.

ID администраторов, требуемые Центру операций

У администратора должны быть допустимые ID и пароль на хаб-сервере для входа в Центр операций. Кроме того, Центру операций назначается ID администратора, чтобы Центр операций мог отслеживать серверы.

Центр операций требует следующие ID администраторов IBM Spectrum Protect:

ID администраторов, зарегистрированные на хаб-сервере
Для входа в Центр операций можно использовать любой ID администратора, зарегистрированный на хаб-сервере. Уровень полномочий ID определяет, какие задачи можно выполнять. Создать ID администраторов можно командой **REGISTER ADMIN**.

Ограничение: Для использования ID администратора в конфигурации с несколькими серверами он должен быть зарегистрирован на хаб-сервере и подчиненных серверах с одинаковыми паролями и уровнями полномочий.

Для управления аутентификацией для этих серверов выберите один из следующих способов:

- Сервер LDAP (Lightweight Directory Access Protocol)
- Функции конфигурирования организации для автоматического распределения изменений определения администратора.

ID администратора мониторинга
При начальном конфигурировании хаб-сервера ID администратора IBM-OC-*имя_сервера* регистрируется с системными полномочиями на хаб-сервере и связывается с начальным паролем, заданным вами. Этот ID, иногда называемый *администратор мониторинга*, предназначен для использования только Центром операций.

Не удаляйте, не блокируйте и не изменяйте этот ID. Тот же ID администратора с тем же паролем регистрируется на добавленных подчиненных серверах. Пароль автоматически изменяется на хаб-сервере и на подчиненных серверах каждые 90 дней. Вам не нужно использовать этот пароль или управлять им.

Ограничение: Центр операций управляет ID и паролем администратора мониторинга на подчиненных серверах, если только вы не используете для управления этими идентификационными данными конфигурацию организации. Дополнительную информацию об использовании конфигурации организации для управления идентификационными данными смотрите в разделе “Советы по проектированию конфигурации хаб-сервера и подчиненных серверов” на стр. 139.

IBM Installation Manager

Центр операций использует IBM Installation Manager - программу установки, которая может использовать удаленные или локальные репозитории программ для установки или обновления многих продуктов IBM.

Если обязательная версия IBM Installation Manager еще не установлена, то она автоматически устанавливается или обновляется при установке Центра операций. Она должна остаться установленной на компьютере, чтобы позже можно было обновить или деинсталлировать Центр операций.

Ниже приведены объяснения некоторых терминов, используемых в IBM Installation Manager:

Предложение
Устанавливаемый модуль программного продукта.

Предложение Центра операций содержит все носители, которые требуются IBM Installation Manager для установки Центра операций.

Пакет
Группа программных компонентов, необходимых для установки предложения.

Пакет Центра операций включает в себя следующие компоненты:

- Программу установки IBM Installation Manager
- Предложение Центра операций

Группа пакетов
Набор пакетов, использующих общий родительский каталог.

Репозиторий
Удаленная или локальная область хранения данных и других ресурсов приложения.

Пакет Центра операций хранится в репозитории в IBM Fix Central.

Каталог общих ресурсов
Каталог, содержащий файлы или модули plugin программ, которые совместно используются пакетами.

IBM Installation Manager хранит в каталоге общих ресурсов связанные с установкой файлы, включая файлы, используемые для отката к предыдущей версии Центр операций.

Контрольный список установки

Прежде чем приступить к установке компонента Центр операций, необходимо проверить определенную информацию, такую как идентификационные данные установки, и определить входные данные, которые нужно предоставить IBM Installation Manager для установки.

В следующем контрольном списке перечислена информация, которую надо проверить или определить, прежде чем приступать к установке Центра операций; в таблице Таблица 28 на стр. 147 дано подробное описание этой информации:

__ Проверьте имя хоста для компьютера, на котором устанавливается Центр операций.

__ Проверьте идентификационные данные для установки.
__ Определите каталог установки Центра операций, если не хотите принимать путь по умолчанию.
__ Определите каталог установки IBM Installation Manager, если не хотите принимать путь по умолчанию.
__ Определите порт, который должен использоваться веб-сервером Центра установки, если не хотите принимать номер порта по умолчанию.
__ Определите пароль для защищенной связи.

Таблица 28. Информация, которую нужно проверить или определить, прежде чем приступать к установке Центра операций

Информация	**Сведения**
Имя хоста для компьютера, на котором нужно установить Центр операций.	Имя хоста должно отвечать следующим критериям: • Оно не должно содержать двухбайтные символы (DBCS) или символы подчеркивания (_). • Имя хоста может содержать символ дефиса (-), но это не должен быть последний символ в имени.
Идентификационные данные для установки	Для установки Центра операций следует использовать следующую учетную запись пользователя: • Пользователь root

Каталог установки Центра операций	Центр операций устанавливается в подкаталог `ui` каталога установки.
	Следующие каталоги - это каталоги установки Центра операций по умолчанию:
	• `/opt/tivoli/tsm`
	Например, если вы используете каталог по умолчанию, то Центр операций устанавливается в следующий каталог:
	`/opt/tivoli/tsm/ui`
	Имя каталога установки должно соответствовать следующим критериям:
	• Имя каталога может содержать не более 128 символов.
	• Имя каталога должно содержать только символы ASCII.
	• Имя каталога не должно содержать не показываемые символы управления.
	• Имя каталога не должно содержать следующие символы:
	`% | < > ' " $ & ; *`

Каталог установки IBM Installation Manager	Следующие каталоги - это каталоги установки IBM Installation Manager по умолчанию: • `/opt/IBM/InstallationManager`

Таблица 28. Информация, которую нужно проверить или определить, прежде чем приступать к установке Центра операций (продолжение)

Информация	**Сведения**
Номер порта, используемый веб-сервером компонента Центр операций.	Номер защищенного (https) порта должен соответствовать следующим критериям: • Этот номер должен быть целым числом в диапазоне 1024 - 65535. • Этот номер не должен уже использоваться или быть выделенным другим программам. Если номер порта не указан, то используется значение по умолчанию 11090. **Советы:** • Хотя надо определить целое число в диапазоне 1024 - 65535, можно позже конфигурировать Центр операций, чтобы использовать стандартный защищенный порт TCP/IP (порт 443). Дополнительную информацию смотрите в разделе “Конфигурирование веб-сервера Центра операций для использования стандартного защищенного порта TCP/IP” на стр. 162. • Если позже вы забудете указанный вами номер порта, найдите его в следующем файле, где *каталог_установки* - это каталог, куда установлен Центр операций: – *каталог_установки*/ui/Liberty/usr/servers/guiServer/bootstrap.properties Файл bootstrap.properties содержит информацию для соединения с сервером IBM Spectrum Protect.

Таблица 28. Информация, которую нужно проверить или определить, прежде чем приступать к установке Центра операций (продолжение)

Информация	**Сведения**
Пароль для защищенной связи	Центр операций использует протокол HTTPS (Hypertext Transfer Protocol Secure) для связи с веб-браузерами. Для компонента Центр операций требуется защищенная связь между сервером и компонентом Центр операций. Для защиты связи нужно добавить сертификат Transport Layer Security (TLS) хаб-сервера в файл склада доверенных сертификатов компонента Центр операций. Файл склада доверенных сертификатов компонента Центр операций 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. При настройке защищенной связи между компонентом Центр операций и хаб-сервером нужно использовать тот же пароль для добавления сертификата хаб-сервера в файл склада доверенных сертификатов. Пароль для склада доверенных сертификатов должен отвечать следующим критериям: • Пароль должен содержать не менее 6 и не более 64 символов. • Пароль должен содержать, как минимум, следующие символы: – Одну заглавную букву (A – Z) – Одну строчную букву (a – z) – Одну цифру (0 – 9) – Два символа, не являющихся алфавитно-цифровыми, которые указаны в следующем ряду: `~ @ # $ % ^ & * _ - + = ` |`  `( ) { } [ ] : ; < > , . ? /`

Глава 9. Установка сервера Центра операций

Центр операций можно установить любым из следующих методов: графический мастер, командная строка в режиме консоли или режим без вывода сообщений.

Прежде чем начать

Чтобы сконфигурировать Центр операций, нужно установить, сконфигурировать и запустить сервер IBM Spectrum Protect. Поэтому перед установкой Центра операций установите подходящий пакет сервера в соответствии с требованиями к версии сервера, приведенными в разделе “Требования для хаб-сервера и подчиненных серверов” на стр. 138.

Центр операций можно установить на компьютер, на котором установлен сервер IBM Spectrum Protect, или на другой компьютер.

Получение пакета установки Центра операций

Пакет установки можно получить с сайта скачивания IBM, например, IBM Passport Advantage или IBM Fix Central.

Об этой задаче

После получения пакета с сайта загрузок IBM вы должны извлечь установочные файлы.

Процедура

Выполните описанные ниже шаги, чтобы извлечь файлы установки компонента Центр операций. В следующих шагах замените *номер_версии* на устанавливаемую вами версию компонента Центр операций.

a. Скачайте один из следующих файлов пакетов в каталог по вашему выбору:
   - *номер_версии*.000-IBM-SPOC-LinuxS390.bin
   - *номер_версии*.000-IBM-SPOC-Linuxx86_64.bin

b. Убедитесь, что у вас есть разрешения на выполнение для файла пакета.

   Если нужно, то измените разрешения для файла, введя следующую команду:

   ```
   chmod a+x имя_пакета.bin
   ```

c. Чтобы извлечь файлы установки, введите следующую команду:

   ```
   ./имя_пакета.bin
   ```

   Самоизвлекающийся файл пакета извлекается в каталог.

Установка Центра операций при помощи графического мастера

Центр операций можно установить или обновить при помощи графического мастера IBM Installation Manager.

Процедура

1. Введите в каталоге, в который вы извлекли файл пакета установки Центра операций, следующую команду:

```
./install.sh
```

2. Выполните инструкции мастера, чтобы установить пакеты IBM Installation Manager и Центра установки.

Дальнейшие действия

Смотрите раздел “Конфигурирование Центра операций” на стр. 157.

Установка Центра операций в режиме консоли

Центр операций можно установить или обновить из командной строки в режиме консоли.

Процедура

1. Запустите из каталога, в который вы извлекли файл пакета установки, следующую программу:

```
./install.sh -c
```

2. Выполните инструкции в консоли, чтобы установить пакеты Installation Manager и Центра установки.

Дальнейшие действия

Смотрите раздел “Конфигурирование Центра операций” на стр. 157.

Установка компонента Центр операций в режиме без вывода сообщений

Центр операций можно установить или обновить в режиме без вывода сообщений. В режиме без вывода сообщений установка не отправляет сообщений на консоль, а сохраняет сообщения и ошибки в файлы журнала.

Прежде чем начать

Чтобы задать входные данные при использовании установки в режиме без вывода сообщений, можно использовать файл ответов. Указанные ниже примеры файлов ответов поставляются в каталоге `input` в том месте, куда был распакован пакет установки:

`install_response_sample.xml`
Используйте этот файл для установки Центра операций.

`update_response_sample.xml`
Используйте этот файл для обновления Центра операций.

Эти файлы содержат значения по умолчанию, которые помогут вам избежать всех ненужных предупреждений. Чтобы воспользоваться этими файлами, выполните приведенные в файлах инструкции.

Если вы хотите настроить файл ответов, вы можете изменить опции, содержащиеся в файле. Информацию о файлах ответов смотрите в разделе Файлы ответов.

Процедура

1. Создайте файл ответов.

   Вы можете изменить пример файла ответов или создать свой собственный.

   Совет: Чтобы сгенерировать файл ответов в ходе установки в режиме консоли, выберите опции установки в режиме консоли. Затем введите на панели **Сводка** `G`, чтобы сгенерировать файл ответов в соответствии с опциями, выбранными ранее.

2. Создайте пароль для склада доверенных сертификатов компонента Центр операций в файле ответов.

   Если вы используете файл `install_response_sample.xml`, добавьте пароль в следующую строку в файле, где *пароль* - это пароль:

   ```
   <variable
   name='ssl.password' value='пароль' />
   ```

   Дополнительную информацию об этом пароле смотрите в разделе “Контрольный список установки” на стр. 146.

   Чтобы зашифровать пароль, выполните инструкции из раздела “Шифрование паролей в файлах ответов установки без вывода сообщений” на стр. 153.

   Совет: Пароль склада доверенных сертификатов не требуется, если вы используете файл `update_response_sample.xml` для обновления компонента Центр операций.
3. Запустите установку без вывода сообщений, введя в каталоге, в который распакован пакет установки, следующую команду. Значение *файл_ответов* соответствует пути и имени файла ответов:

   - ```
     ./install.sh -s -input файл_ответов
     -acceptLicense
     ```

Дальнейшие действия

Смотрите раздел “Конфигурирование Центра операций” на стр. 157.

Шифрование паролей в файлах ответов установки без вывода сообщений

Для дополнительной защиты при установке Центра операций в режиме без вывода сообщений можно зашифровать пароль в файле ответов. В поле ключа данных в файле ответов можно указать только один пароль (зашифрованный или незашифрованный).

Прежде чем начать

Откройте IBM Installation Manager. В каталоге, где установлен IBM Installation Manager, перейдите в подкаталог `eclipse`. Положение подкаталога по умолчанию:

```
/opt/IBM/InstallationManager/eclipse
```

Процедура

Чтобы зашифровать пароль в файле ответов, который используется для установки Центра операций в режиме без вывода сообщений, и убедитесь, что в поле ключа данных используется только один пароль, выполните следующее:

1. Если вы устанавливаете Центр операций от имени пользователя root, перейдите в подкаталог tools. Положение подкаталога tools по умолчанию:

   ```
   /opt/IBM/InstallationManager/eclipse/tools
   ```

   Если вы устанавливаете Центр операций как пользователь без полномочий root, перейдите в следующий подкаталог:

   ```
   /home/пользователь_не_root/IBM/InstallationManager/eclipse/tools
   ```

   где *пользователь_не_root* - это ID пользователя экземпляра.
2. Введите следующую команду в виде одной строки:
   ```

```
./IBMIM -silent -noSplash encryptString строка_для_шифрования
>зашифрованный_пароль
```

где *строка_для_шифрования* -это зашифрованное значение, а *зашифрованный_пароль* - это файл, содержащий зашифрованное значение.

3. Откройте зашифрованный файл паролей и скопируйте значение в поле ключа данных файла ответов. Затем удалите зашифрованный файл паролей, закомментировав его.
4. Чтобы удалить незашифрованный пароль из поля ключа данных, выполните следующее:
   a. Закомментируйте незашифрованный пароль (USER.SSL_PASSWORD), чтобы строка пароля была похожа на следующий пример:

   ```
   <!-- <data key='user.SSL_PASSWORD' value='${ssl.password}'/> -->
   ```

   b. Удалите теги комментариев из зашифрованного пароля (user.SSL_PASSWORD_ENCRYPTED), чтобы строки пароля были похожи на следующий пример:

   ```
   <data key='user.enableSP800_131' value='${enable.SP800131a}'/>
    <data key='user.SSL_PASSWORD_ENCRYPTED' value='${ssl.password.encrypted}'/>
   ```

   Ограничение: Используйте только одно значение в поле ключа данных в файле ответа, либо пароль user.SSL_PASSWORD, либо пароль user.SSL_PASSWORD_ENCRYPTED. Надо закомментировать тот, который вы не используете, или вы получите сообщение об ошибке, а установка завершится неудачно.

Пример

С помощью инструмента командной строки Installation Manager зашифруйте пароль passw0rd. Сохраните зашифрованное значение в файле my_pwd.txt. Введите следующую команду:

```
./IBMIM -silent -noSplash encryptString passw0rd > my_pwd.txt
```

где файл my_pwd.txt содержит зашифрованное значение, *rbN1IaMAWYYtQxLf6KdNyA==*:

```
<variable name='ssl.password.encrypted' value=' rbN1IaMAWYYtQxLf6KdNyA==' />
```

Глава 10. Обновление компонента Центр операций

Центр операций можно обновить любым из следующих методов: графический мастер, командная строка в режиме консоли или режим без вывода сообщений.

Прежде чем начать

Перед обновлением Центра операций ознакомьтесь с требованиями к системе и с контрольным списком установки. У новой версии Центра операций могут быть дополнительные или другие требования по сравнению с версией, которую вы используете в настоящий момент.

Об этой задаче

Инструкции по обновлению Центра операций совпадают с инструкциями по установке Центра операций за следующими исключениями:

- Используйте функцию **Обновить** программы IBM Installation Manager, а не функцию **Установить**.

  Совет: В IBM Installation Manager термин *обновить* (update) означает поиск и установку обновлений и исправлений для установленных программных пакетов. В этом контексте термины *update* и *upgrade* - это синонимы.
- Если вы обновляете Центр операций в режиме без вывода сообщений, то вы можете пропустить шаг создания пароля для файла склада доверенных сертификатов.

Глава 11. Начинаем работу с компонентом Центр операций

Перед тем, как вы сможете управлять средой хранения при помощи Центра операций, необходимо его сконфигурировать.

Об этой задаче

После установки Центра операций выполните следующие базовые действия конфигурирования:

1. Определите хаб-сервер.
2. Добавьте подчиненные серверы.
3. При необходимости сконфигурируйте оповещения по электронной почте на хаб-сервере и подчиненных серверах.

Рисунок 1 на стр. 157 иллюстрирует конфигурацию Центра операций.

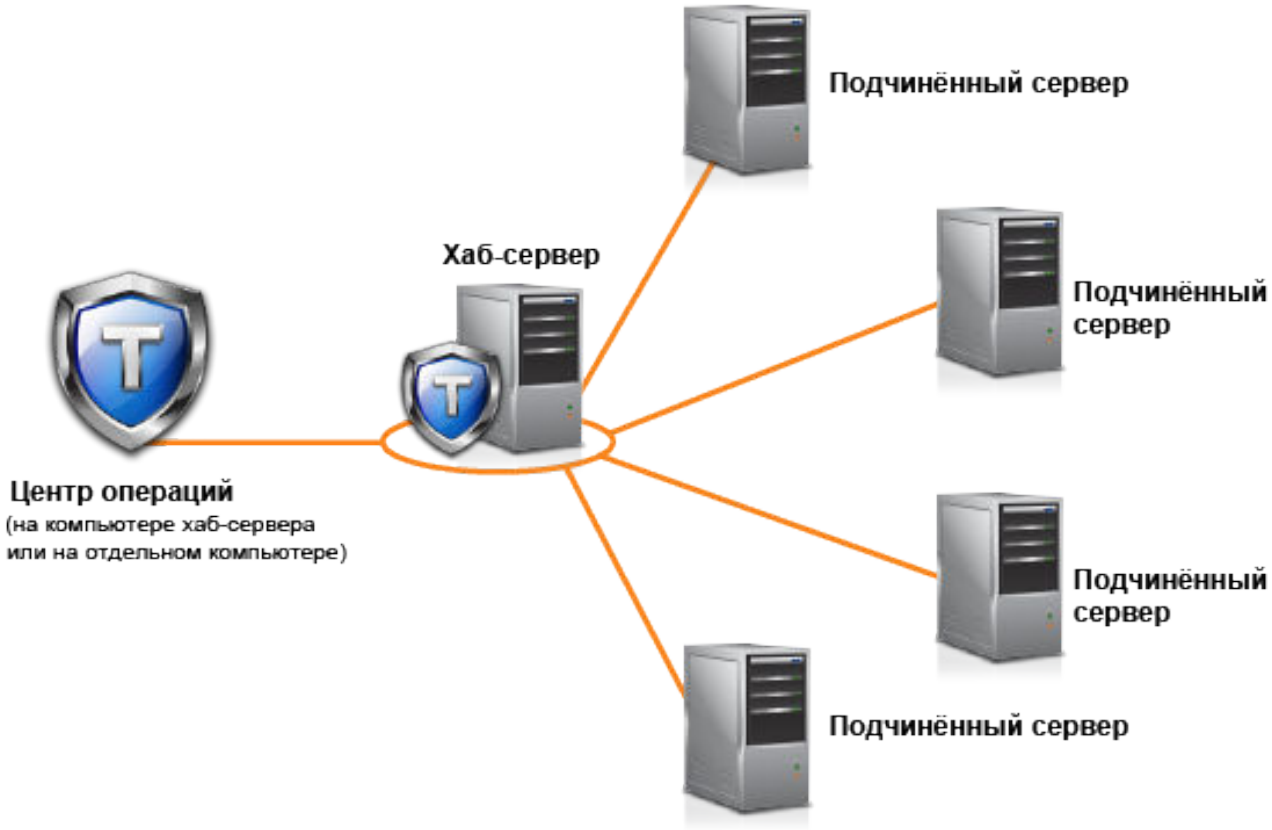


Рисунок 1. Пример конфигурации Центра операций с хаб-сервером и подчиненными серверами

Конфигурирование Центра операций

Если вы открываете Центр операций впервые, то его нужно сконфигурировать для управления средой хранения. Вы должны связать Центр операций с сервером IBM Spectrum Protect, заданным в качестве хаб-сервера. После этого можно подключить дополнительные серверы IBM Spectrum Protect как подчиненные серверы.

Назначение хаб-сервера

Когда вы в первый раз соединяетесь с Центром операций, вы должны указать, какой сервер IBM Spectrum Protect является хаб-сервером.

Прежде чем начать

Для компонента Центр операций требуется защищенная связь между хаб-сервером и компонентом Центр операций. Для защиты связи нужно добавить сертификат Transport Layer Security (TLS) хаб-сервера в файл склада доверенных сертификатов компонента Центр операций. Дополнительную информацию смотрите в разделе “Защита связи между Центром операций и хаб-сервером с использованием самоподписанных сертификатов” на стр. 164.

Процедура

В браузере введите следующий адрес, где *имя_хоста* - это имя компьютера, на котором установлен Центр операций, а *защищенный_порт* - это номер порта, который Центр операций использует для связи HTTPS на этом компьютере:

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

Советы:

- В URL учитывается регистр символов. Например, убедитесь, что вы ввели "oc" строчными буквами, как это показано.
- Дополнительную информацию о номере порта смотрите в разделе Контрольный список установки.
- Если вы подключаетесь к Центру операций впервые, то 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
- Если срок хранения записи события сервера меньше 14 дней, то для него автоматически задается значение 14 дней, если сервер конфигурируется как хаб-сервер.

Дальнейшие действия

Если в среде есть несколько серверов IBM Spectrum Protect, то добавьте на хаб-сервер остальные серверы как подчиненные серверы.

Внимание: Не изменяйте имя сервера после того, как он сконфигурирован в качестве хаб-сервера или подчиненного сервера.

Добавление подчиненного сервера

После конфигурирования хаб-сервера для Центра операций можно добавить к этому хаб-серверу один или несколько подчиненных серверов.

Прежде чем начать

Связь между подчиненным сервером и хаб-сервером должна быть защищена с использованием протокола Transport Layer Security (TLS). Для защиты связи добавьте сертификат подчиненного сервера в файл доверенных сертификатов хаб-сервера.

Процедура

1. Щелкните в панели меню Центра операций по **Серверы**.

Откроется страница **Серверы**.

В таблице на странице **Серверы** состоянием сервера может быть "Не отслеживается" Это состояние означает, что хотя администратор и определил этот сервер на хаб-сервере при помощи команды **DEFINE SERVER**, этот сервер еще не сконфигурирован в качестве подчиненного сервера.

2. Выполните одно из следующих действий:
   - Щелкните по серверу, чтобы выделить его, и щелкните в панели меню таблицы по **Отслеживать подчиненный**.
   - Если сервера, который вы хотите добавить, нет в таблице, а защищенная связь SSL/TLS не требуется, то щелкните по **+ Подчиненный** в панели меню таблицы.
3. Задайте нужную информацию и выполните действия в мастере конфигурирования подчиненных серверов.

   Совет: Если срок хранения записи события сервера меньше 14 дней, то для него автоматически задается значение 14 дней, если сервер конфигурируется как подчиненный сервер.

Отправка оповещений администраторам по электронной почте

Оповещение - это уведомление о проблеме на сервере IBM Spectrum Protect; оповещение инициализируется сообщением сервера. Оповещения могут быть показаны в Центре операций; сервер может отправлять оповещения администраторам по электронной почте.

Прежде чем начать

Прежде чем конфигурировать уведомления по электронной почте об оповещениях для администраторов, убедитесь, что выполнены следующие требования:

- Для отправки и получения оповещений по электронной почте требуется сервер SMTP; у сервера, который отправляет оповещения по электронной почте, должен быть доступ к серверу SMTP.

  Совет: Если Центр операций установлен на отдельном компьютере, этому компьютеру не нужен доступ к серверу SMTP.
- У администратора должна быть системные полномочия для конфигурирования отправки уведомлений по электронной почте.

Об этой задаче

Уведомление по электронной почте отправляется только для первого возникновения оповещения. Кроме того, если оповещение сгенерировано до того, как вы сконфигурировали уведомление по электронной почте, для этого оповещения не отправляется уведомление по электронной почте.

Уведомления по электронной почте можно сконфигурировать следующими способами:

- Отправка уведомлений для отдельных оповещений
- Отправка сводки оповещений

Сводка оповещений содержит информацию о текущих оповещениях. В сводке указаны общее число оповещений, общее число активных и неактивных оповещений, самое старое оповещение, самое новое оповещение и наиболее часто встречающееся оповещение.

Можно указать до трех администраторов, получающих сводки оповещений по электронной почте. Сводки оповещений отправляются примерно раз в час.

Процедура

Чтобы сконфигурировать уведомления по электронной почте об оповещениях для администраторов, выполните следующие действия на каждом хаб-сервере и подчиненном сервере, от которых вы хотите получать оповещения по электронной почте.

1. Чтобы проверить, включен ли мониторинг оповещений, введите следующую команду:

```
QUERY MONITORSETTINGS
```

2. Если в выводе этой команды говорится, что мониторинг оповещений выключен, введите следующую команду. В ином случае переходите к следующему шагу.

```
SET ALERTMONITOR ON
```

3. Чтобы включить отправку уведомлений по электронной почте, введите следующую команду:

```
SET ALERTEMAIL ON
```

4. Чтобы определить сервер SMTP, используемый для отправки уведомлений по электронной почте, введите следующую команду:

```
SET ALERTEMAILSMTPHOST имя_хоста
```

5. Чтобы указать номер порта для сервера SMTP, введите следующую команду:

```
SET ALERTEMAILSMTPPORT номер_порта
```

Номер порта по умолчанию - 25.

6. Чтобы указать адрес электронной почты отправителя оповещений, введите следующую команду:

```
SET ALERTEMAILFROMADDR адрес_электронной_почты
```

7. Для каждого ID администратора, который должен получать уведомления по электронной почте, введите одну из следующих команд, чтобы активировать уведомления по электронной почте и задать адрес электронной почты:

```
REGISTER ADMIN имя_администратора ALERT=YES EMAILADDRESS=адрес_электронной_почты
```

```
UPDATE ADMIN имя_администратора ALERT=YES EMAILADDRESS=адрес_электронной_почты
```

8. Выберите любую из следующих опций (или обе этих опции) и укажите ID администраторов, которые должны получать уведомления по электронной почте:

   - Отправка уведомлений для отдельных оповещений

     Для указания или изменения ID администраторов, которые должны получать уведомления по электронной почте для отдельного оповещения, введите одну из следующих команд:

     ```
     DEFINE ALERTTRIGGER номер_сообщения
     ADmin=имя_администратора_1,имя_администратора_2
     ```

     ```
     UPDATE
     ALERTTRIGGER номер_сообщения ADDadmin=имя_администратора_3
     DELadmin=имя_администратора_1
     ```

     Совет: На странице **Сконфигурировать оповещения** Центра операций можно выбрать администраторов, которые будут получать уведомления по электронной почте.

   - Отправка сводки оповещений

     Чтобы задать или изменить ID администраторов для получения сводки оповещений по электронной почте, введите следующую команду:

     ```
     SET ALERTSUMMARYTOADMINS имя_администратора1,имя_администратора2,имя_администратора3
     ```

   Если вы хотите получать сводки оповещений, но не хотите получать уведомления об отдельных оповещениях, то сделайте следующее:

   a. Приостановите уведомления об отдельных оповещениях, как описано в разделе “Временная приостановка отправки оповещений по электронной почте” на стр. 161.

b. Убедитесь, что соответствующий ID администратора указан в следующей команде:

```
SET ALERTSUMMARYTOADMINS имя_администратора1,имя_администратора2,имя_администратора3
```

Отправка оповещений нескольким администраторам по электронной почте

В следующем примере показаны команды, которые инициируют отправку по электронной почте всех оповещений для сообщения ANR1075E администраторам myadmin, djadmin и csadmin:

```
SET ALERTMONITOR ON
SET ALERTEMAIL ON
SET ALERTEMAILSMTPHOST mymailserver.domain.com
SET ALERTEMAILSMTPPORT 450
SET ALERTEMAILFROMADDR srvadmin@mydomain.com
UPDATE ADMIN myadmin ALERT=YES EMAILADDRESS=myaddr@anycompany.com
UPDATE ADMIN djadmin ALERT=YES EMAILADDRESS=djaddr@anycompany.com
UPDATE ADMIN csadmin ALERT=YES EMAILADDRESS=csaddr@anycompany.com
DEFINE ALERTTRIGGER anr0175e ADMIN=myadmin,djadmin,csadmin
```

Временная приостановка отправки оповещений по электронной почте

Бывают ситуации, когда нужно временно приостановить оповещения по электронной почте. Например, вы хотите получать сводни оповещений, но приостановить уведомления об отдельных оповещениях, или вы хотите приостановить отправку оповещений по электронной почте, если администратор находится в отпуске.

Прежде чем начать

Сконфигурируйте уведомления по электронной почте для администраторов (смотрите раздел “Отправка оповещений администраторам по электронной почте” на стр. 159).

Процедура

Приостановите уведомления по электронной почте для отдельных оповещений или для сводок оповещений.

- Приостановить уведомления для отдельных оповещений

  Для этого можно воспользоваться любым из следующих способов:

  Команда UPDATE ADMIN

  Чтобы отключить уведомления по электронной почте для администратора, введите следующую команду:

  ```
  UPDATE ADMIN
  имя_администратора ALERT=NO
  ```

  Чтобы позднее снова включить уведомления по электронной почте, введите следующую команду:

  ```
  UPDATE ADMIN имя_администратора ALERT=YES
  ```

  Команда UPDATE ALERTTRIGGER

  Чтобы отключить отправку администратору определенного оповещения, введите следующую команду:

  ```
  UPDATE ALERTTRIGGER
  номер_сообщения DELADMIN=имя_администратора
  ```

  Чтобы запустить отправку администратору этого оповещения, введите следующую команду:

  ```
  UPDATE ALERTTRIGGER номер_сообщения ADDADMIN=имя_администратора
  ```

- Приостановить уведомления о сводках оповещений

Чтобы отключить отправку администратору сводок оповещений, удалите этого администратора из списка в следующей команде:

```
SET ALERTSUMMARYTOADMINS имя_администратора1,имя_администратора2,имя_администратора3
```

Если в предыдущей команде указан ID администратора, этот администратор получает сводки оповещений по электронной почте, даже если для соответствующего ID администратора приостановлены отдельные оповещения.

Добавление настроенного текста в окно входа в систему

Вы можете добавить пользовательский текст (например, Условия использования программы вашей организации) в окно входа в Центр операций, чтобы пользователи Центра операций видели этот текст перед вводом имени пользователя и пароля.

Процедура

Чтобы добавить пользовательский текст в экран входа в систему, сделайте следующее:

1. На компьютере с установленным компонентом Центр операций перейдите в следующий каталог, где *каталог_установки* представляет собой каталог, в котором установлен Центр операций:

   каталог_установки/ui/Liberty/usr/servers/guiServer
2. Создайте в каталоге файл `loginText.html`, содержащий текст, который вы хотите добавить в экран входа в систему.

   Текст, содержащий специальные символы и символы не ASCII, должен быть в кодировке UTF-8.
3. Проверьте добавленный текст в окне входа в Центр операций.

   Чтобы открыть Центр операций, введите в веб-браузере следующий адрес, где *имя_хоста* - это имя компьютера, на котором установлен Центр операций, а *защищенный_порт* - это номер порта, который Центр операций использует для связи HTTPS на этом компьютере:

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

Конфигурирование веб-сервера Центра операций для использования стандартного защищенного порта TCP/IP

Порт 443 - это стандартный порт для защищенной связи веб-браузера. Если пользователи должны получать доступ к Центру операций через брандмауэр, можно сконфигурировать Центр операций для взаимодействия через этот стандартный порт. Таким образом можно постараться не открывать другой порт в брандмауэре.

Об этой задаче

При установке Центра операций номер порта по умолчанию для защищенной связи между веб-сервером Центра операций и веб-браузерами - 11090. Этот порт по умолчанию можно принять во время установки, либо можно указать другой номер порта в диапазоне 1024 - 65535. Задать номер порта меньше 1024 в момент установки нельзя, так как эти порты зарезервированы для конкретных сетевых служб.

После установки Центра операций веб-сервер принимает на указанном порту запросы от веб-браузеров. Если пользователи не могут открыть центр операций, потому что порт заблокирован брандмауэром, то администратор должен открыть порт, чтобы позволить браузерам соединяться. В некоторых производственных средах использование системного порта 443 может оказаться более эффективным. Поскольку этот системный порт зарезервирован для защищенного просмотра веб-страниц, он, вероятно, уже открыт в брандмауэре. Хотя порт 443 нельзя указать во время установки, его можно указать после установки.

Процедура

Чтобы сконфигурировать веб-сервер Центра операций для использования порта 443, выполните следующие шаги после установки Центра операций:

1. Остановите веб-сервер Центра операций.

   Инструкции по остановке веб-сервера смотрите в разделе “Запуск и остановка веб-сервера” на стр. 184.
2. Перейдите в следующий каталог, где *каталог_установки* - это каталог, в котором установлен компонент Центр операций:

   каталог_установки/ui/Liberty/usr/servers/guiServer
3. Откройте файл `bootstrap.properties`, который содержит свойство, задающее порт, используемый веб-сервером Центра операций для защищенной связи.
4. Обновите свойство `tsm.https.port`, указав порт 443:

   ```
   tsm.https.port=443
   ```
5. Сохраните и закройте файл `bootstrap.properties`.
6. Запустите веб-сервер Центра операций.

   Надо запустить Центр операций от имени пользователя root. Если не запустить Центр операций от имени пользователя root, то Центр операций не сможет соединяться через порт 443.

   Инструкции по запуску веб-сервера Центра операций смотрите в разделе “Запуск и остановка веб-сервера” на стр. 184.

Дальнейшие действия

Уведомите пользователей о том, что Центр операций использует стандартный защищенный порт TCP/IP. Как правило, пользователь открывает Центр операций в своем браузере, включив номер порта в URL. Поскольку порт 443 - это значение по умолчанию для защищенной связи веб-браузера, пользователям не нужно указывать номер порта в URL. Вместо этого можно использовать следующий URL, где *имя_хоста* - это имя компьютера, на котором установлен Центр операций:

```
https:имя_хоста/oc/
```

Инструкции по открытию Центра операций смотрите в разделе “Открытие Центра операций” на стр. 185.

Как включить службы REST

Приложения, которые используют службы Representational State Transfer (REST), могут запрашивать среду хранения и управлять средой хранения, соединяясь с центром операций.

Об этой задаче

Включите эту функцию, чтобы разрешить службам REST взаимодействовать с хаб-серверами и подчиненными серверами путем отправки вызовов по следующему адресу:

```
https://имя_хоста_цо:порт/oc/api
```

где *имя_хоста_цо* - это сетевое имя или IP-адрес хост-системы Центра операций, а *порт* - это номер порта Центра операций. Номер порта по умолчанию - 11090.

Чтобы получить информацию о службах REST, доступных для Центра операций, смотрите техническое примечание http://www-01.ibm.com/support/docview.wss?uid=swg21997347 или введите следующий вызов REST:

```
https://имя_хоста_цо:порт/oc/api/help
```

Процедура

1. В строке меню Центра операций установите указатель мыши на значок параметров и щелкните по **Параметры**.
2. На странице Общие включите переключатель **Включить API REST администрирования**.
3. Нажмите кнопку **Сохранить**.

Конфигурирование для защищенной связи

Центр операций использует протокол HTTPS (Hypertext Transfer Protocol Secure) для связи с Web-браузерами. Протокол Transport Layer Security (TLS) защищает связь между Центром операций и хаб-сервером, а также между хаб-сервером и связанными подчиненными серверами.

Об этой задаче

Для защищенной связи между сервером IBM Spectrum Protect и компонентом Центр операций, а также между хаб-сервером и подчиненными серверами требуется TLS версии 1.2 или новее.

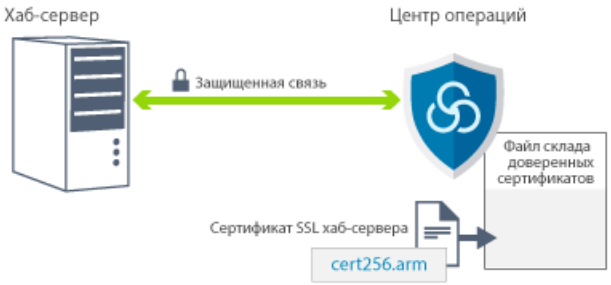
Защита связи между Центром операций и хаб-сервером с использованием самоподписанных сертификатов

Для защиты связи между компонентом Центр операций и хаб-сервером нужно добавить сертификат Transport Layer Security (TLS) хаб-сервера в файл склада доверенных сертификатов компонента Центр операций.

Прежде чем начать

Файл склада доверенных сертификатов компонента Центр операций - это контейнер сертификатов, доступ к которому может получить Центр операций. При установке компонента Центр операций вы должны создать 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 склада доверенных сертификатов. Если вы не помните этот пароль, вы должны будете в этот момент создать заново и сконфигурировать файл склада доверенных сертификатов. Инструкции смотрите в разделе Удаление и переназначение пароля файла склада доверенных сертификатов Центра операций.

На следующем рисунке показаны компоненты для настройки соединения Secure Sockets Layer (SSL) между хаб-сервером и компонентом Центр операций.



Об этой задаче

В этой процедуре описаны шаги по реализации защищенной связи с использованием самоподписанных сертификатов. Если вы используете сертификаты, подписанные центром сертификации (certificate authority, CA), смотрите раздел Защита связи между Центром операций и хаб-сервером с использованием сертификатов, подписанных центром сертификации.

Процедура

1. Остановите веб-сервер Центра операций
2. Перейдите в командную строку операционной системы, в которой установлен компонент Центр операций.
3. Добавьте сертификат в файл доверенных сертификатов компонента Центр операций, используя утилиту **iKeycmd** или утилиту **iKeyman**.

   Утилита **iKeyman** - это интерфейс командной строки, а утилита **iKeyman** - это графический пользовательский интерфейс IBM Key Management.

   Утилиты **iKeycmd** и **iKeyman** нужно запускать от имени пользователя root.

   Чтобы добавить сертификат TLS, используя интерфейс командной строки, выполните следующие шаги:

   a) Перейдите в следующий каталог, где *каталог_установки* - это каталог, в котором установлен компонент Центр операций:

   - *каталог_установки*/ui/jre/bin

   b) Введите команду **iKeycmd**, чтобы добавить сертификат `cert256.arm` сервера в склад доверенных сертификатов компонента Центр операций.

   ```
   ikeycmd -cert -add
   - db /каталог_установки/ui/Liberty/usr/servers/guiServer/gui-truststore.jks
   -file /каталог_экземпляра_сервера/cert256.arm
   -label 'описание_метки'
   -pw 'пароль' -type jks -format ascii -trust enable
   ```

   Здесь используются следующие обозначения:

   каталог_установки
   Каталог установки компонента Центр операций.

   каталог_экземпляра_сервера
   Каталог экземпляра сервера IBM Spectrum Protect.

   описание метки
   Описание, заданное вами для метки.

   пароль
   Пароль, созданный вами при установке компонента Центр операций. Чтобы переустановить пароль, деинсталлируйте компонент Центр операций, удалите файл `.jks` и переустановите компонент Центр операций.

   Чтобы добавить сертификат, используя окно **IBM Key Management**, выполните следующие шаги:

   a) Перейдите в следующий каталог, где *каталог_установки* - это каталог, в котором установлен компонент Центр операций:

   - *каталог_установки*/ui/jre/bin

   b) Откройте окно **Управление ключами IBM**, введя следующую команду:

   ```
   ikeyman
   ```

   c) Выберите **Файл базы данных ключей** > **Открыть**.

   d) В окне **Открыть** щелкните по **Просмотр** и перейдите в следующий каталог, где *каталог_установки* - это каталог, в котором установлен Центр операций:

   - *каталог_установки*/ui/Liberty/usr/servers/guiServer

   e) Выберите в каталоге `guiServer` файл `gui-truststore.jks`.

   f) Щелкните по **Открыть**, а затем по **OK**.

   g) Введите пароль для файла склада доверенных сертификатов и щелкните по **OK**.

h) В области **Содержимое базы данных ключей** окна **Управление ключами IBM** щелкните по стрелке и выберите в списке **Сертификаты подписывающих**.

i) Щелкните по **Добавить**.

j) В окне **Открыть** щелкните по **Обзор** и перейдите в каталог экземпляра хаб-сервера. В этом каталоге содержится сертификат `cert256.arm`.

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

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

- *каталог_установки*`/ui/Liberty/usr/servers/guiServer`

ii) В окне **Открыть** перейдите в каталог`guiServer`.

k) Выберите сертификат `cert256.arm`.

Совет: Выбранный вами сертификат должен быть задан в качестве сертификата по умолчанию в файле базы данных ключей хаб-сервера.

l) Щелкните по **Открыть**, а затем по **OK**.

m) Введите метку для сертификата.
Например, задайте имя хаб-сервера.

n) Нажмите кнопку **OK**.

Сертификат SSL хаб-сервера будет добавлен в файл склада доверенных сертификатов, и его метка появится в области **Содержимое базы данных ключей** в окне **Управление ключами IBM**.

o) Закройте окно **Управление ключами IBM**.

4. Запустите веб-сервер Центра операций.
5. 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. Введите номер порта, заданный опцией TCPADMINPORT или SSLTCPADMINPORT.

   Если компонент Центр операций сконфигурирован, вы можете посмотреть содержимое файла `serverConnection.properties`, чтобы проверить информацию о соединении. Файл `serverConnection.properties` находится в следующем каталоге компьютера, где установлен компонент Центр операций:

   - *каталог_установки*`/ui/Liberty/usr/servers/guiServer`

Дальнейшие действия

Чтобы узнать, как настроить связь TLS между хаб-сервером и подчиненным сервером, смотрите раздел “Защита связи между хаб-сервером и подчиненным сервером” на стр. 168.

Задачи, связанные с данной

“Удаление и переназначение пароля файла склада доверенных сертификатов Центра операций” на стр. 182
Чтобы настроить защищенную связь между компонентом Центр операций и хаб-сервером, вы должны знать пароль файла склада доверенных сертификатов компонента Центр операций. Этот пароль создается при установке компонента Центр операций. Если вы не знаете пароль, можно удалить и переназначить его.

Защита связи между Центром операций и хаб-сервером с использованием сертификатов, подписанных центром сертификации

Если вы используете для защиты хаб-сервера сертификат, подписанный центром сертификации (Certificate Authority, CA), файлы корневого и промежуточного сертификатов центра сертификации,

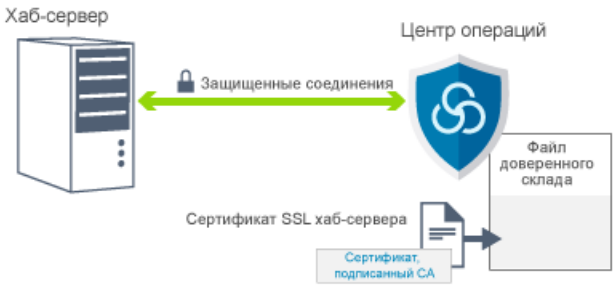
отправленные центром сертификации для использования на хаб-сервере, должны быть добавлены в файл доверенных сертификатов компонента Центр операций.

Прежде чем начать

Убедитесь, что выполнены следующие предварительные требования:

- Файл склада доверенных сертификатов компонента Центр операций - это контейнер сертификатов, доступ к которому может получить Центр операций. При установке компонента Центр операций вы должны создать 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 склада доверенных сертификатов. Если вы не помните этот пароль, вы должны будете в этот момент создать заново и сконфигурировать файл склада доверенных сертификатов. Инструкции смотрите в разделе “Удаление и переназначение пароля файла склада доверенных сертификатов Центра операций” на стр. 182.
- Вы получили из центра сертификации необходимые для соединения с сервером сертификаты, подписанные центром сертификации, и установили их на сервере. Смотрите раздел Конфигурирование сервера для приема соединений SSL.

На следующем рисунке показаны компоненты для настройки соединения Secure Sockets Layer (SSL) между хаб-сервером и компонентом Центр операций.



Об этой задаче

Чтобы импортировать с хаб-сервера в Центр операций корневой и промежуточный сертификаты центра сертификации для каждого сервера IBM Spectrum Protect, выполните следующие шаги:

Совет: Если вы используете самоподписанные сертификаты, которые устанавливаются по умолчанию, смотрите раздел “Защита связи между Центром операций и хаб-сервером с использованием самоподписанных сертификатов” на стр. 164.

Процедура

1. Перейдите в командную строку операционной системы, в которой установлен компонент Центр операций.
2. В командной строке перейдите в положение склада ключей:

   каталог_установки`/ui/Liberty/usr/servers/guiServer`

   Где *каталог_установки* - это каталог, в котором установлен компонент Центр операций.
3. Скопируйте файлы корневого сертификата CA и промежуточного сертификата CA в этот каталог.

   Совет: Файлы сертификатов были ранее скопированы в каталог хаб-сервера.
4. Остановите веб-сервер Центр операций, как описано в разделе “Запуск и остановка веб-сервера” на стр. 184.
5. Создайте резервную копию файла склада доверенных сертификатов компонента Центр операций на случай, если вам потребуется вернуться к исходной версии. Имя файла склада доверенных сертификатов компонента Центр операций - `gui-truststore.jks`.
6. Чтобы выполните действия по получению сертификата, подписанного центром сертификации, используйте одну из следующих команд:

- Команда **ikeyman**: Смотрите раздел “Получение подписанного сертификата при помощи IBM Key Management” на стр. 174 и перейдите к шагам по получению подписанного сертификата.
- Команда **ikeycmd**: Смотрите раздел “Получение подписанного сертификата при помощи команды ikeycmd” на стр. 181 и перейдите к шагам по получению подписанного сертификата.

7. Запустите веб-сервер компонента Центр операций.

Дальнейшие действия

Чтобы узнать, как настроить связь TLS между хаб-сервером и подчиненным сервером, следуйте инструкциям в разделе “Защита связи между хаб-сервером и подчиненным сервером” на стр. 168.

Задачи, связанные с данной

“Получение подписанного сертификата” на стр. 174
Центр сертификации должен послать вам файл сертификата, добавляемый к файлу склада доверенных сертификатов.

Защита связи между хаб-сервером и подчиненным сервером

Чтобы защитить связь между хаб-сервером и подчиненным сервером с использованием протокола Transport Layer Security (TLS), нужно задать для хаб-сервера сертификат подчиненного сервера и сертификат хаб-сервера - для подчиненного сервера. Кроме того, нужно сконфигурировать Центр операций для мониторинга подчиненного сервера.

Об этой задаче

Хаб-сервер получает информацию об оповещениях и состоянии от подчиненного сервера и показывает эту информацию в компоненте Центр операций. Чтобы получить информацию о состоянии и оповещениях от подчиненного сервера, сертификат подчиненного сервера нужно добавить в файл доверенных сертификатов хаб-сервера. Кроме того, нужно сконфигурировать Центр операций для мониторинга подчиненного сервера.

Чтобы включить другие функции компонента Центр операций, например, автоматическое внедрение обновлений клиента, сертификат хаб-сервера нужно добавить в файл доверенных сертификатов подчиненного сервера.

Процедура

1. Выполните следующие шаги, чтобы задать сертификат подчиненного сервера для хаб-сервера:
   a) На подчиненном сервере перейдите в каталог экземпляра подчиненного сервера.
   b) Проверьте сертификаты в файле базы данных ключей подчиненного сервера. Введите следующую команду:

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

   c) Передайте безопасным способом файл `cert256.arm` подчиненного сервера на хаб-сервер.
   d) На хаб-сервере перейдите в каталог экземпляра хаб-сервера.
   e) Задайте сертификат подчиненного сервера на хаб-сервере. Введите указанную ниже команду в каталоге экземпляра хаб-сервера, где *имя_подчиненного_сервера* - это имя подчиненного сервера, а *подчиненный_cert256.arm* - имя файла сертификата подчиненного сервера:

   ```
   gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii -trust enable
    -label имя_подчиненного_сервера -file подчиненный_cert256.arm
   ```

2. Выполните следующие шаги, чтобы задать сертификат хаб-сервера для подчиненного сервера:
   a) На хаб-сервере перейдите в каталог экземпляра хаб-сервера.
   b) Проверьте сертификаты в файле базы данных ключей подчиненного сервера. Введите следующую команду:

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

c) Передайте безопасным способом файл `cert256.arm` хаб-сервера на подчиненный сервер.

d) На подчиненном сервере перейдите в каталог экземпляра подчиненного сервера.

e) Задайте сертификат хаб-сервера для подчиненного сервера. Введите указанную ниже команду из каталога экземпляра подчиненного сервера, где *имя_хаб_сервера* - это имя хаб-сервера, а *хаб_cert256.arm* - это имя файла сертификата хаб-сервера:

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii -trust enable
 -label имя_хаб_сервера -file хаб_cert256.arm
```

3. Перезапустите хаб-сервер и подчиненный сервер.
4. Выполните следующие шаги, чтобы задать подчиненный сервер для хаб-сервера и хаб-сервер для подчиненного сервера:

   a) Введите на хаб-сервере и на подчиненном сервере следующие команды:

   ```
   SET SERVERPASSWORD пароль_сервера
   SET SERVERHLADDRESS ip_адрес
   SET SERVERLLADDRESS порт_tcp
   ```

   b) На хаб-сервере введите команду **DEFINE SERVER** в соответствии со следующим примером:

   ```
   DEFINE SERVER имя_подчиненного_сервера HLA=адрес_подчиненного_сервера
    LLA=spoke_SSLTCPADMINPort SERVERPA=пароль_подчиненного_сервера
   ```

   c) На подчиненном сервере введите команду **DEFINE SERVER** в соответствии со следующим примером:

   ```
   DEFINE SERVER имя_хаб_сервера HLA=адрес_хаба
    LLA=hub_SSLTCPADMINPort SERVERPA=пароль_хаб_сервера
   ```

   Совет: По умолчанию, взаимодействия с сервером шифруются за исключением случаев, когда сервер отправляет или принимает данные объектов. Данные объектов отправляются и принимаются с использованием TCP/IP. Если выбрать опцию, запрещающую шифровать данные объекта, производительность сервера будет аналогична взаимодействиям в сеансе TCP/IP, и сеанс будет защищен. Чтобы зашифровать все взаимодействия с указанным сервером, даже если сервер отправляет или принимает данные объектов, задайте параметр SSL=YES в команде **DEFINE SERVER**.

5. Выполните следующие шаги, чтобы сконфигурировать Центр операций для мониторинга подчиненного сервера:

   a) В строке меню компонента Центр операций щелкните по **Серверы**.

   Подчиненный сервер будет находиться в состоянии "Без мониторинга". Это состояние означает, что, хотя этот сервер задан для хаб-сервера с использованием команды **DEFINE SERVER**, сервер еще не сконфигурирован как подчиненный сервер.

   b) Щелкните по подчиненному серверу, чтобы выделить элемент, и щелкните по **Отслеживать подчиненный**.

Конфигурирование связи SSL между компонентом Центр операций и веб-браузерами

При установке компонента Центр операций генерируется самоподписанный цифровой сертификат, который затем используется для сеансов веб-браузера. По желанию можно использовать не самоподписанный сертификат, а сертификат подписанный сторонним сертификатором.

Об этой задаче

Компонент Центр операций всегда использует протокол HTTPS для взаимодействий с веб-браузерами. Все взаимодействия между браузером и Центром операций шифруются с использованием версии 1.2 или новее протокола TLS.

По умолчанию для создания защищенного соединения между браузером и компонентом Центр операций используется самоподписанный сертификат. Поскольку сертификат является самоподписанным сертификатом, веб-браузер не может проверить идентичность сервера и выдает предупреждение. Самоподписанные сертификаты обычно используются для веб-сайтов внутренней сети, где риск перехвата соединения и взаимодействия с обезличенным сервером не может считаться серьезной угрозой. Предупреждение защиты браузера можно обойти и использовать самоподписанный сертификат, либо можно заменить самоподписанный сертификат сертификатом от доверенного сертификатора (certificate authority, CA).

Чтобы использовать самоподписанный сертификат, дальнейшее конфигурирование не требуется.

Чтобы использовать сертификат, подписанный CA, необходимо выполнить ряд шагов:

Процедура

1. Создайте требование подписи сертификата.
2. Отправьте запрос на подписание сертификата сертификатору для подписания.
3. Добавьте сертификат в файл склада доверенных сертификатов компонента Центр операций.

Создание требования подписи сертификата

Чтобы получить сертификат, подписанный третьей стороной, нужно создать требование подписи сертификата (certificate signing request, CSR) и отправить его в центр сертификации.

Прежде чем начать

Файл склада доверенных сертификатов компонента Центр операций - это контейнер сертификатов SSL/TLS, доступ к которому может получить Центр операций. Файл склада доверенных сертификатов 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 работать с файлом склада доверенных сертификатов, надо знать пароль склада доверенных сертификатов. Если вы не помните этот пароль, выполните инструкции из раздела “Удаление и переназначение пароля файла склада доверенных сертификатов Центра операций” на стр. 182.

Процедура

Чтобы создать CSR, сделайте следующее:

1. В командной строке перейдите в положение склада ключей:

   каталог_установки/ui/Liberty/usr/servers/guiServer
2. Создайте требование сертификата, используя команду **ikeyman** или команду **ikeycmd**. Команда **ikeyman** открывает графический пользовательский интерфейс IBM Key Management, а **ikeycmd** работает в интерфейсе командной строки.

   Совет: Возможно, вам потребуется указать полный путь к команде **ikeyman** или **ikeycmd**. Команды расположены в следующем каталоге, где *каталог_установки* представляет каталог, в который устанавливается Центр операций:

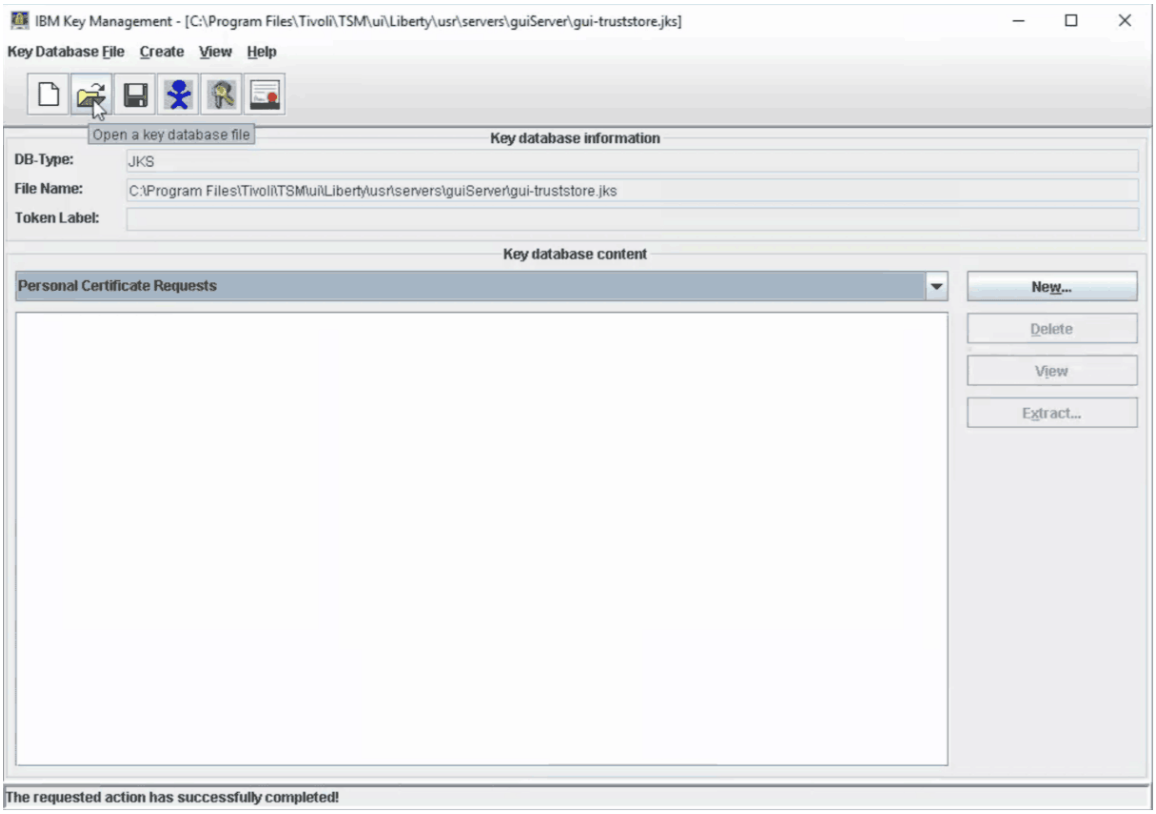
   каталог_установки/ui/jre/bin

   - Чтобы создать требование о сертификате с помощью графического пользовательского интерфейса **ikeyman**, выполните следующие шаги:

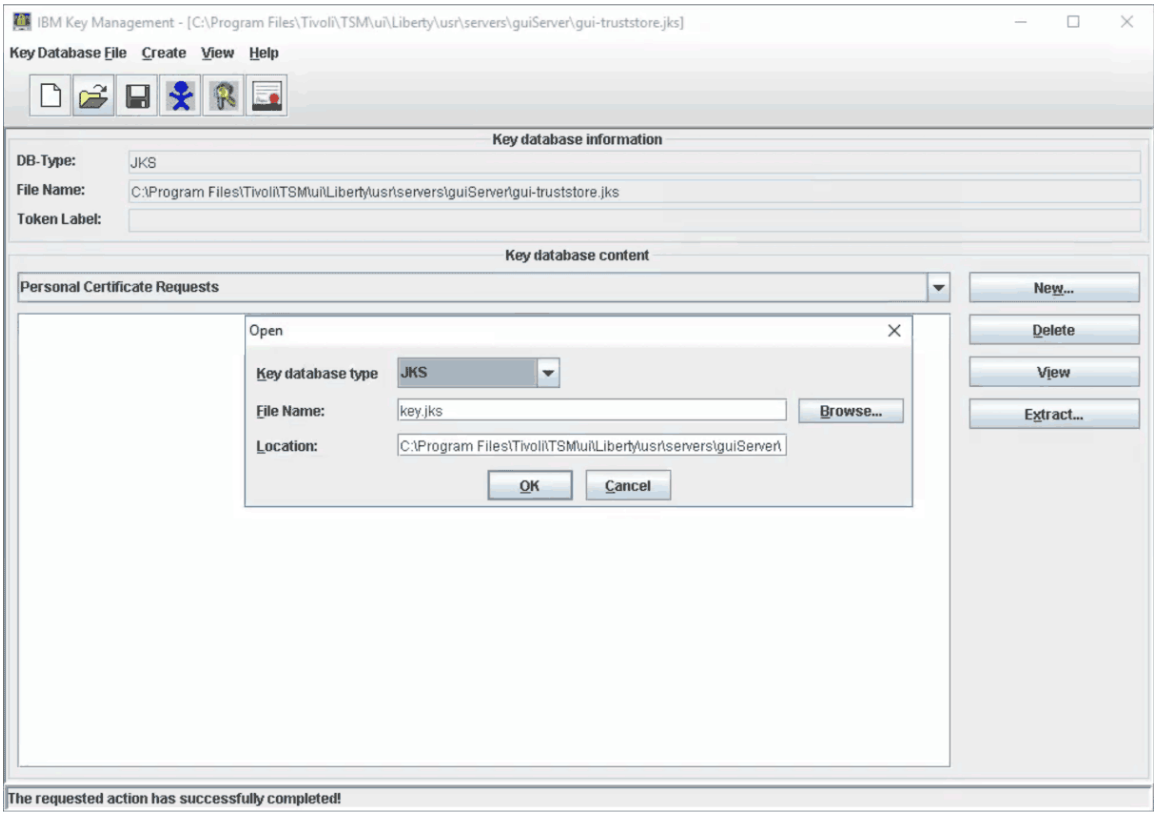
a. Откройте инструмент Управление ключами IBM, введя следующую команду:

```
ikeyman
```

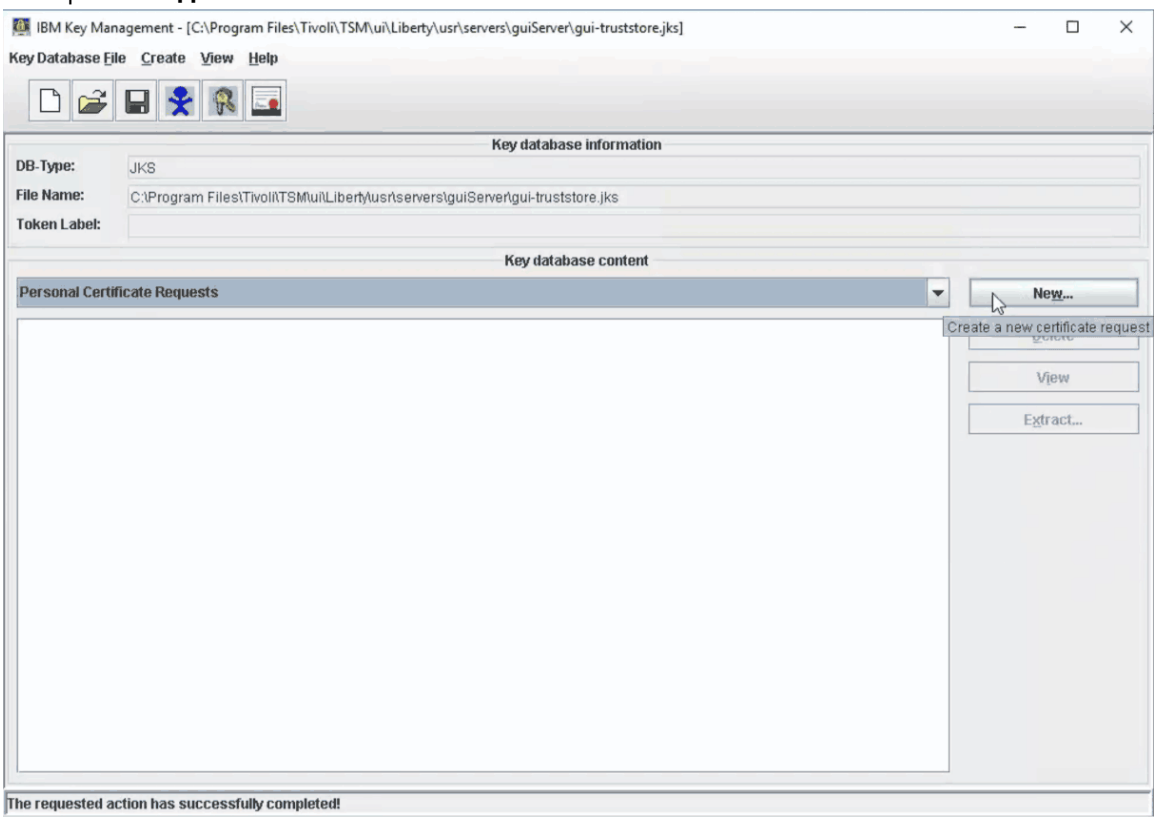
b. Выберите **Файл базы данных ключей** > **Открыть**.



В окне **Открыть** щелкните по **Обзор**, чтобы открыть каталог, и выберите файл `gui-truststore.jks`. Нажмите кнопку **OK**.



c. Создайте требование сертификата. В области **Содержимое базы данных ключей** выберите **Создать**.



d. В диалоговом окне Создать новый ключ и требование сертификата заполните поля, как этого требуют центр сертификации и ваша организация. Задайте следующую информацию:

Метка ключа
Задайте уникальную метку для сертификата в файле склада доверенных сертификатов. Имя метки, например, *имя-сертификата-пользователя*, идентифицирующее сертификат на складе сертификатов.

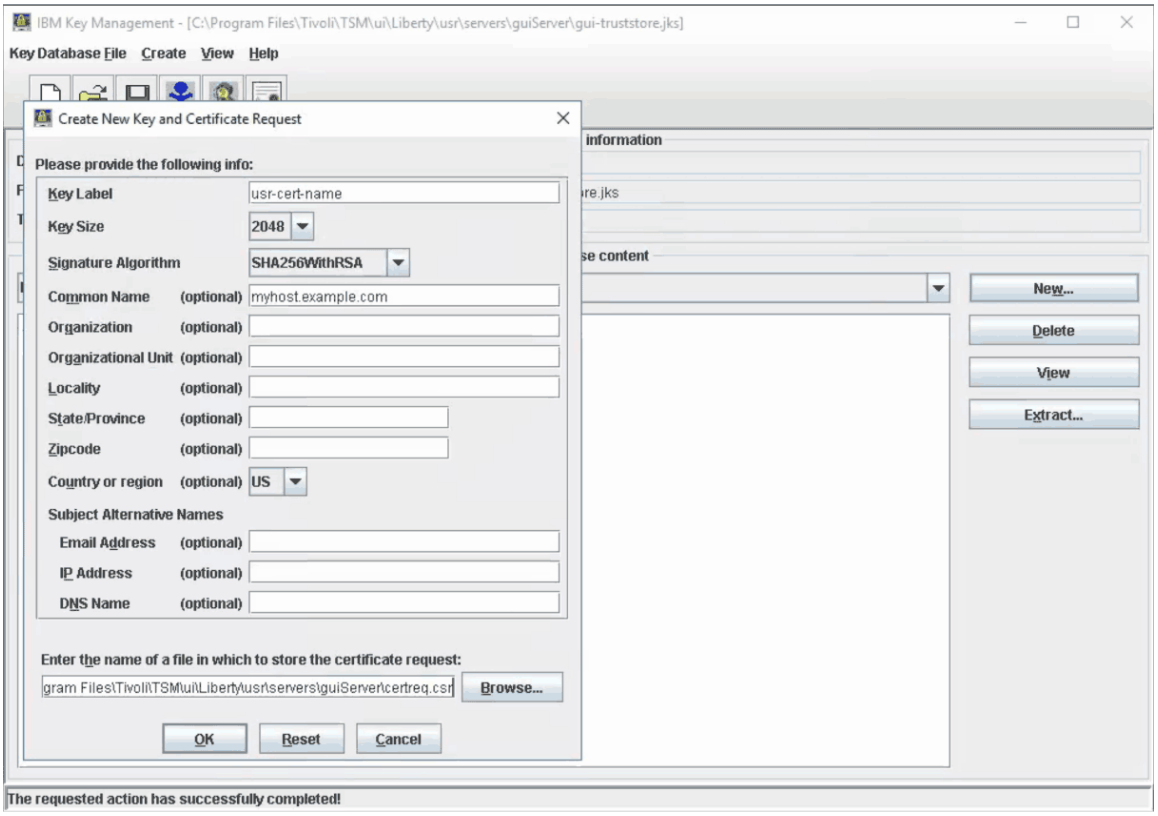
Размер ключа
Выберите размер ключа, не меньше 2048 бит.

Алгоритм сигнатуры
Выберите **SHA256WithRSA**.

Общее имя
Укажите полное доменное имя (fully qualified domain name, FQDN) системы в сети, в которой установлен компонент Центр операций.

Напоминание: FQDN для системы в вашей сети используется в URL для Центра операций в вашей системе. Этот URL применяется в браузере для доступа к Центру операций.

Введите имя файла, в котором следует сохранить требование о сертификате.
Укажите файл с именем `certreq.csr` в каталоге `guiServer`.



e. Закройте окно **Открыть**.

- Чтобы создать требование сертификата, используя команду **ikeycmd**, введите следующую команду:

```
ikeycmd -certreq -create -db gui-truststore.jks -size 2048
-sig_alg SHA256WithRSA -dn "CN=myhost.example.com" -file certreq.csr -label имя-
сертификата-пользователя
-san_dnsname myhost.example.com,myhost
-san_ipaddr 192.0.2.1,192.0.2.2
```

Здесь используются следующие обозначения:

-dn "CN=*myhost.example.com*"
Задает отличительное имя. Вводится как строка в кавычках, содержащая спецификацию CN=*myhost.example.com*, где *myhost.example.com* задает FQDN системы в сети, где установлен Центр операций.

Напоминание: FQDN для системы в вашей сети используется в URL для Центра операций в вашей системе. Этот URL применяется в браузере для доступа к Центру операций.

-label *имя-сертификата-пользователя*
Задает уникальную метку *имя-сертификата-пользователя* для сертификата в файле склада доверенных сертификатов.

-san_dnsname *myhost.example.com,myhost* (необязательно)
Указывает имена сервера доменных имен (DNS) системы, где установлен Центр операций. Значения `CN` и `dnsname` обычно совпадают.

-san_ipaddr *192.0.2.1,192.0.2.2* (необязательно)
Задает IP-адрес системы, в которой установлен Центр операций.

Отправка требования подписи сертификата в центр сертификации

После создания файла требования сертификата (`certreq.csr`) надо отправить его в центр сертификации для получения подписи. Следуйте инструкциям от центра сертификации.

Получение подписанного сертификата

Центр сертификации должен послать вам файл сертификата, добавляемый к файлу склада доверенных сертификатов.

Процедура

Чтобы получить подписанный сертификат, выполните следующие шаги:

1. В командной строке перейдите в положение склада ключей:
   каталог_установки`/ui/Liberty/usr/servers/guiServer`
2. Скопируйте в этот каталог файлы, полученные от CA. Эти файлы включают в себя корневой сертификат CA, промежуточные сертификаты CA (если они есть) и подписанные сертификаты для компонента Центр операций.
3. Остановите веб-сервер Центр операций, как описано в разделе “Запуск и остановка веб-сервера” на стр. 184.
4. Создайте резервную копию склада доверенных сертификатов Центра операций на случай, если вам потребуется вернуться к исходному складу доверенных сертификатов. Имя склада доверенных сертификатов Центра операций - `gui-truststore.jks`.
5. Чтобы выполните действия по получению подписанного сертификата, используйте одну из следующих команд:
   - Команда **ikeyman**: Выполните действия, описанные в разделе “Получение подписанного сертификата при помощи IBM Key Management” на стр. 174.
   - Команда **ikeycmd**: Выполните действия, описанные в разделе “Получение подписанного сертификата при помощи команды ikeycmd” на стр. 181.

Получение подписанного сертификата при помощи IBM Key Management

Можно использовать для управления ключами сертификатов и получения подписанного сертификата графический пользовательский интерфейс - инструмент IBM Key Management.

Процедура

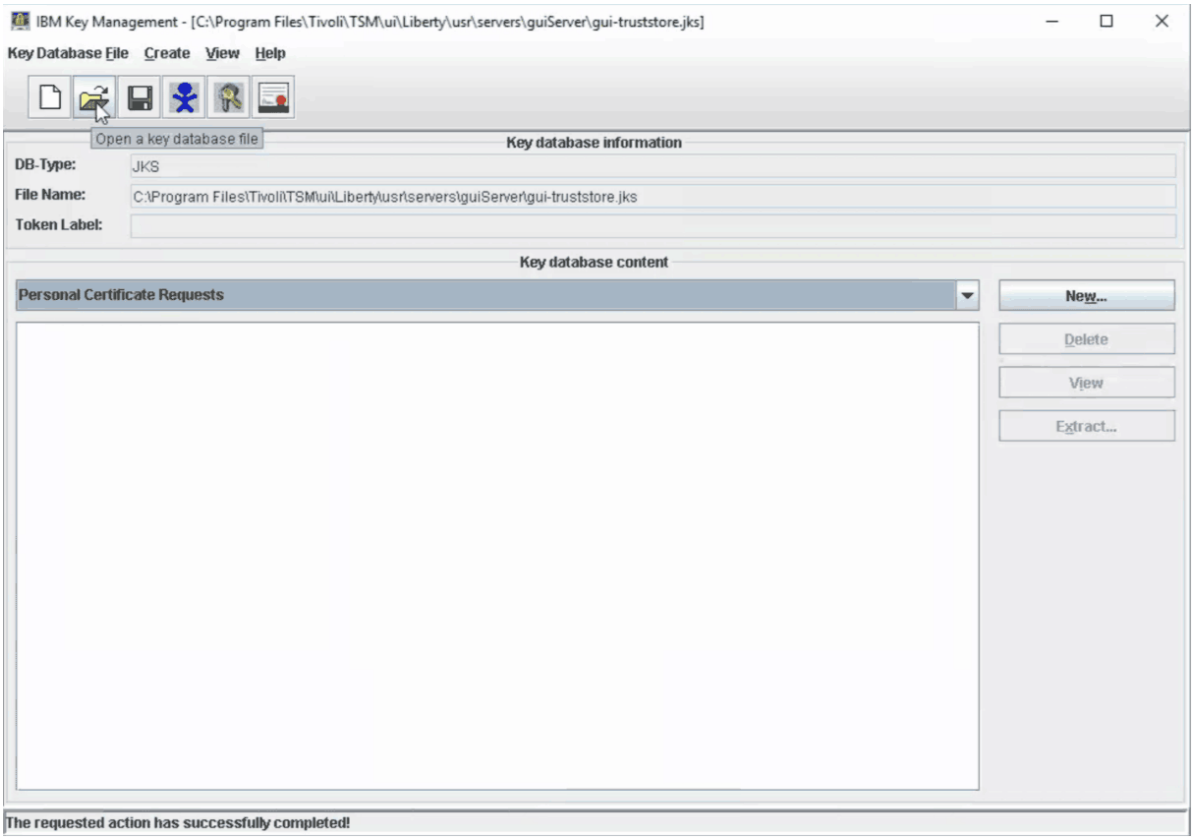
1. Убедитесь, что персональный подписанный сертификат находится в подходящем каталоге, введя команду **ikeyman**. Выполните следующие шаги:
   a) Откройте инструмент Управление ключами IBM, введя следующую команду:

```
ikeyman
```

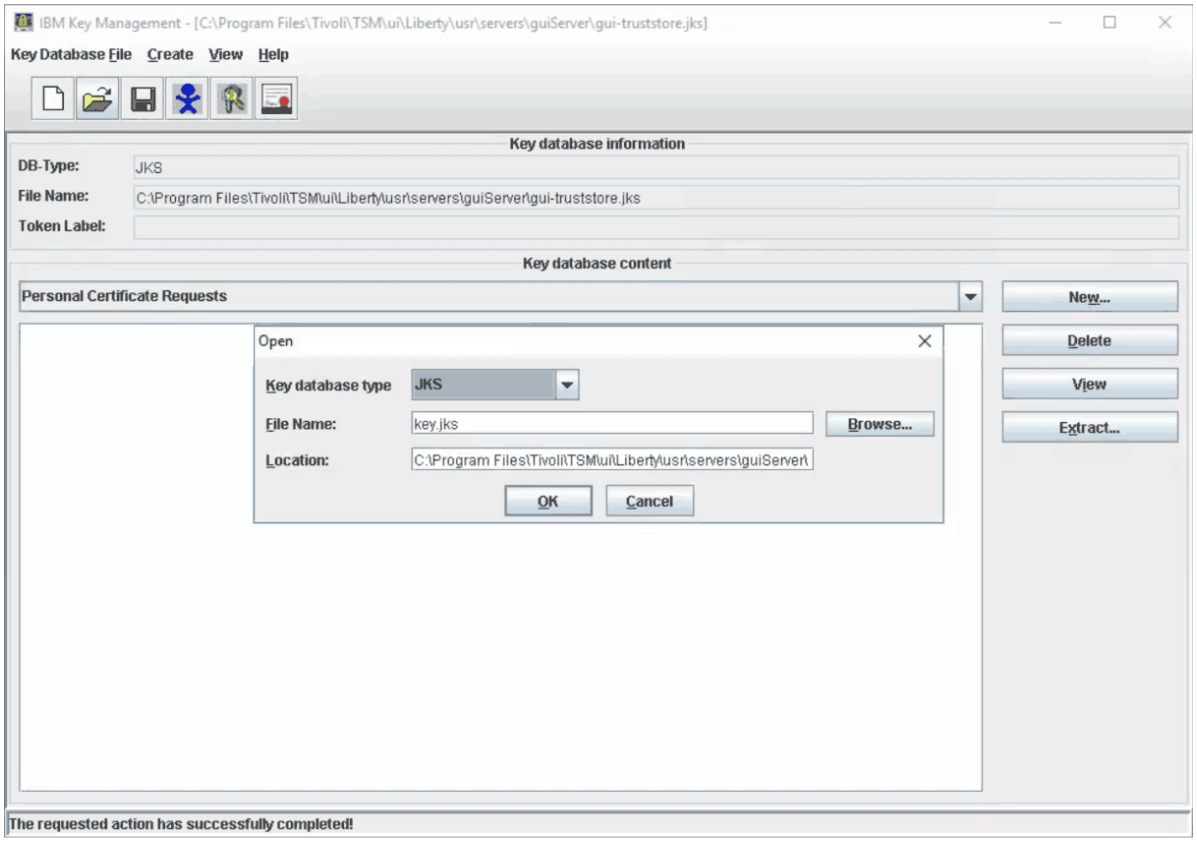
Совет: Возможно, вам потребуется указать полный путь к команде **ikeyman**. Команды расположены в следующем каталоге, где *каталог_установки* представляет каталог, в который устанавливается Центр операций:

каталог_установки/ui/jre/bin

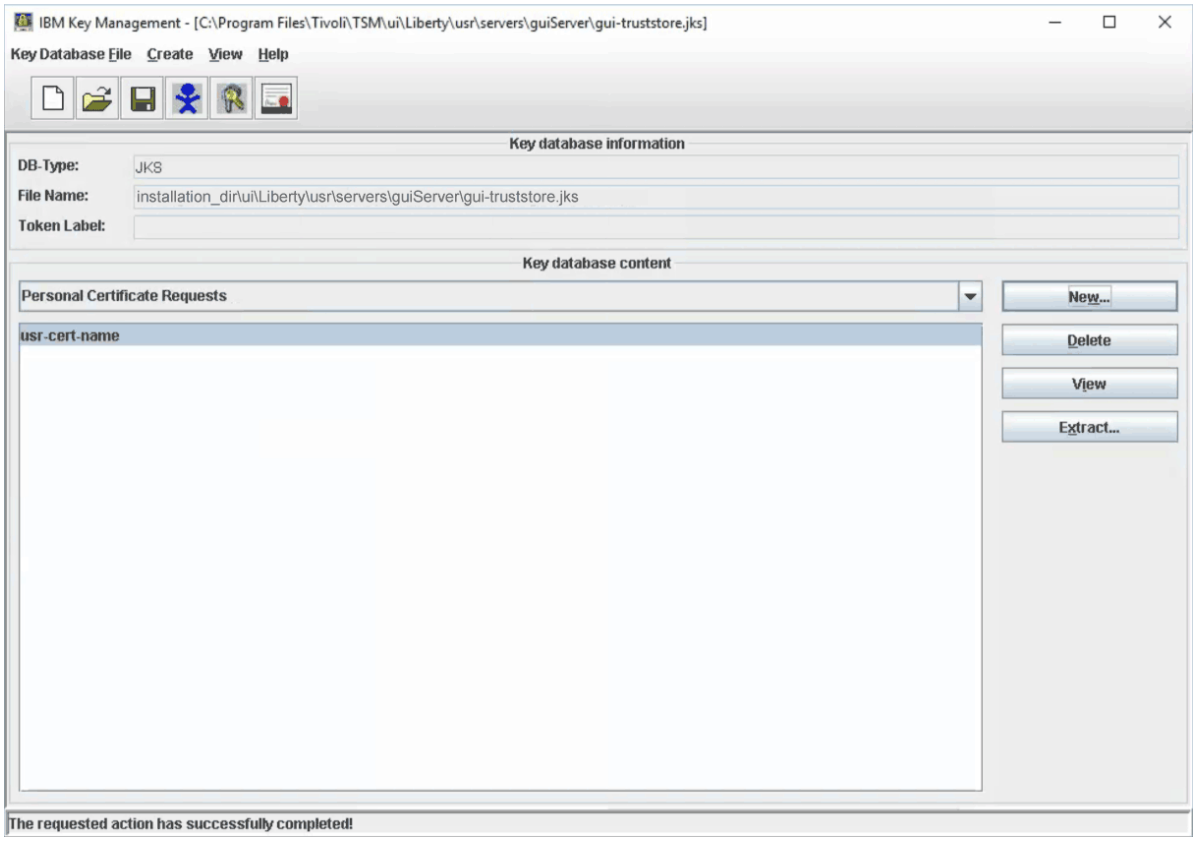
b) Выберите **Файл базы данных ключей** > **Открыть**.



В диалоговом окне **Открыть** щелкните по **Обзор**, чтобы открыть каталог, и выберите файл `gui-truststore.jks`. Нажмите кнопку **OK**.



c) В области **Содержимое базы данных ключей** выберите **Требования персональных сертификатов** убедитесь, что выводится метка **имя-сертификата-пользователя**.

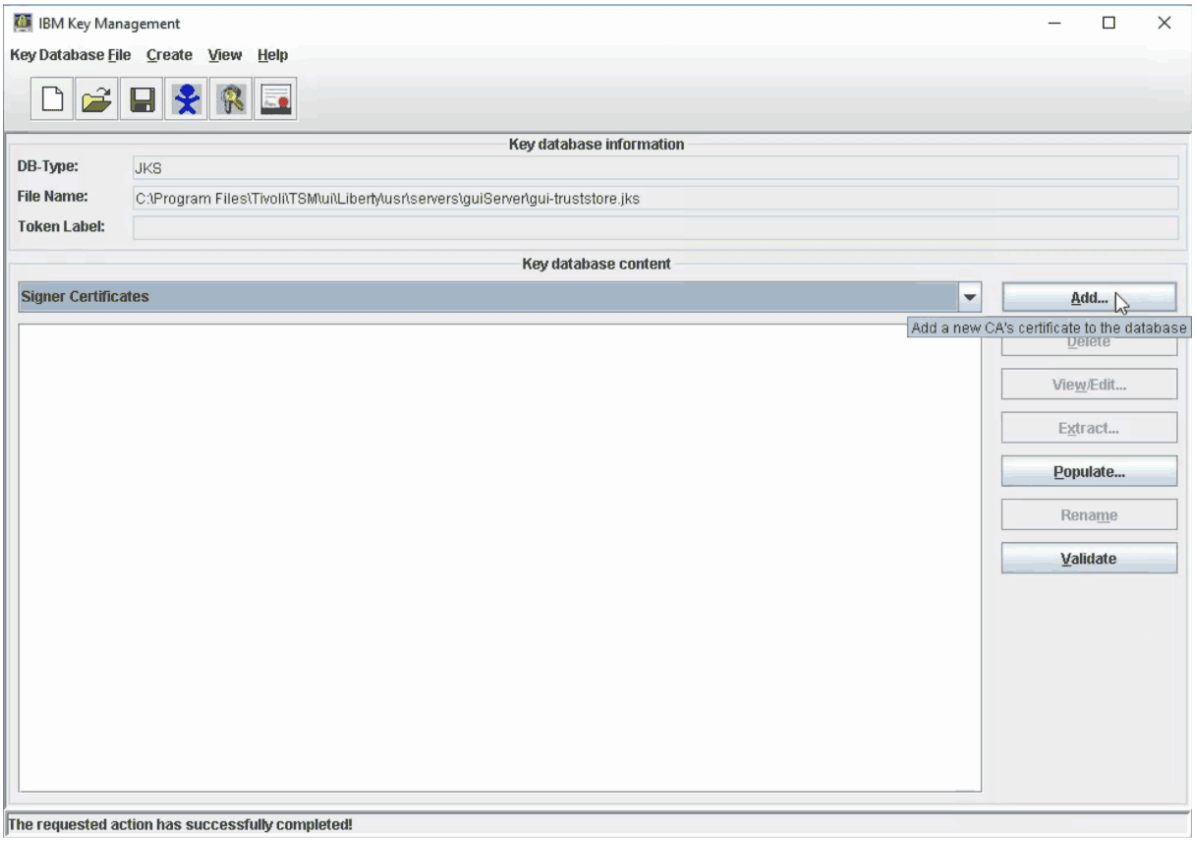


2. Добавьте в файл склада доверенных сертификатов корневой сертификат CA и все промежуточные сертификаты. Если вы получили промежуточные сертификаты от CA, перед

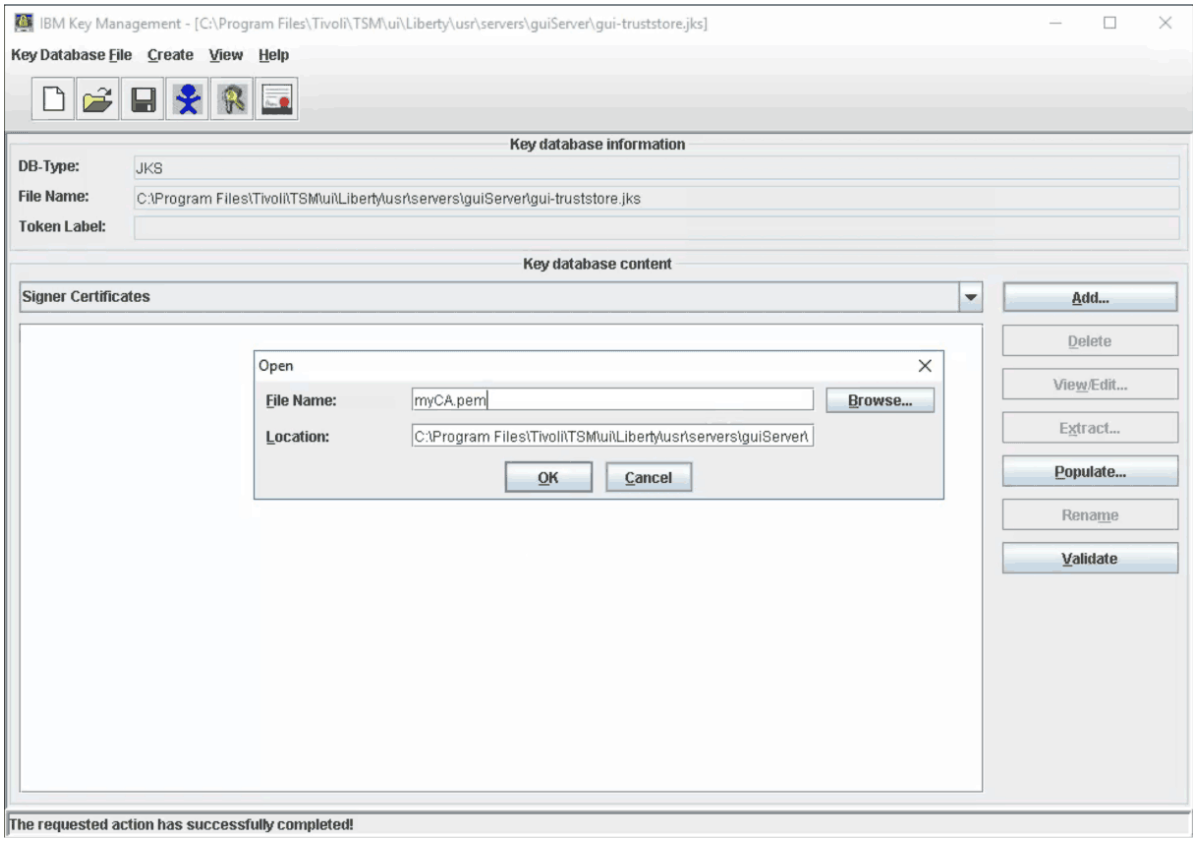
добавлением корневого сертификата CA нужно добавить каждый промежуточный сертификат в файл склада доверенных сертификатов. Выполните описанные ниже шаги для каждого промежуточного сертификата и для корневого сертификата CA.

Важное замечание: CA отправляет один корневой сертификат, подписанный сертификат и, возможно, один или несколько промежуточных сертификатов. В зависимости от CA эти сертификаты могут находиться в одном или в нескольких файлах. Если вы получили сертификаты в одном файле, надо извлечь эти сертификаты как отдельные файлы. Если вы не уверены, как извлечь эти сертификаты, обратитесь в ваш CA.

a) В области **Содержимое базы данных ключей** выберите **Сертификаты подписавшего** и нажмите кнопку **Добавить**.

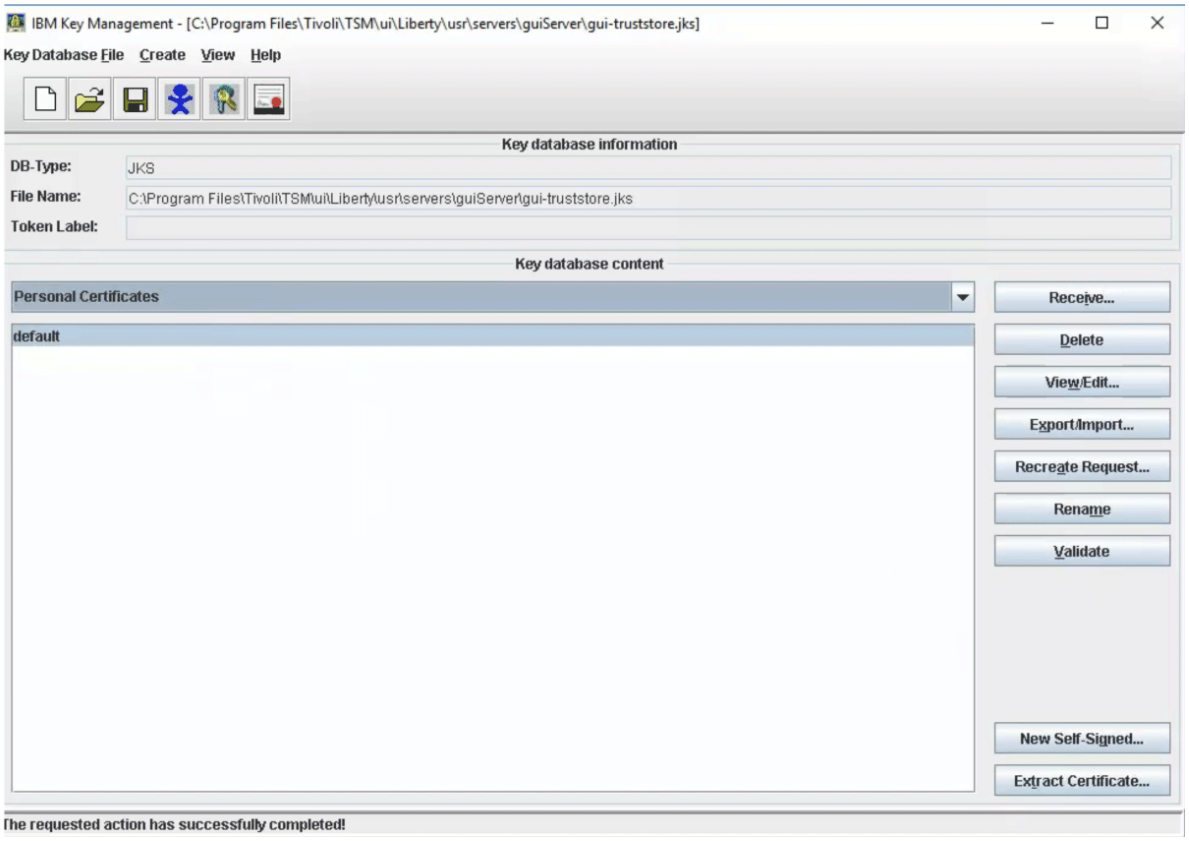


b) В диалоговом окне Открыть укажите корневой сертификат CA или промежуточный сертификат и нажмите кнопку **OK**.

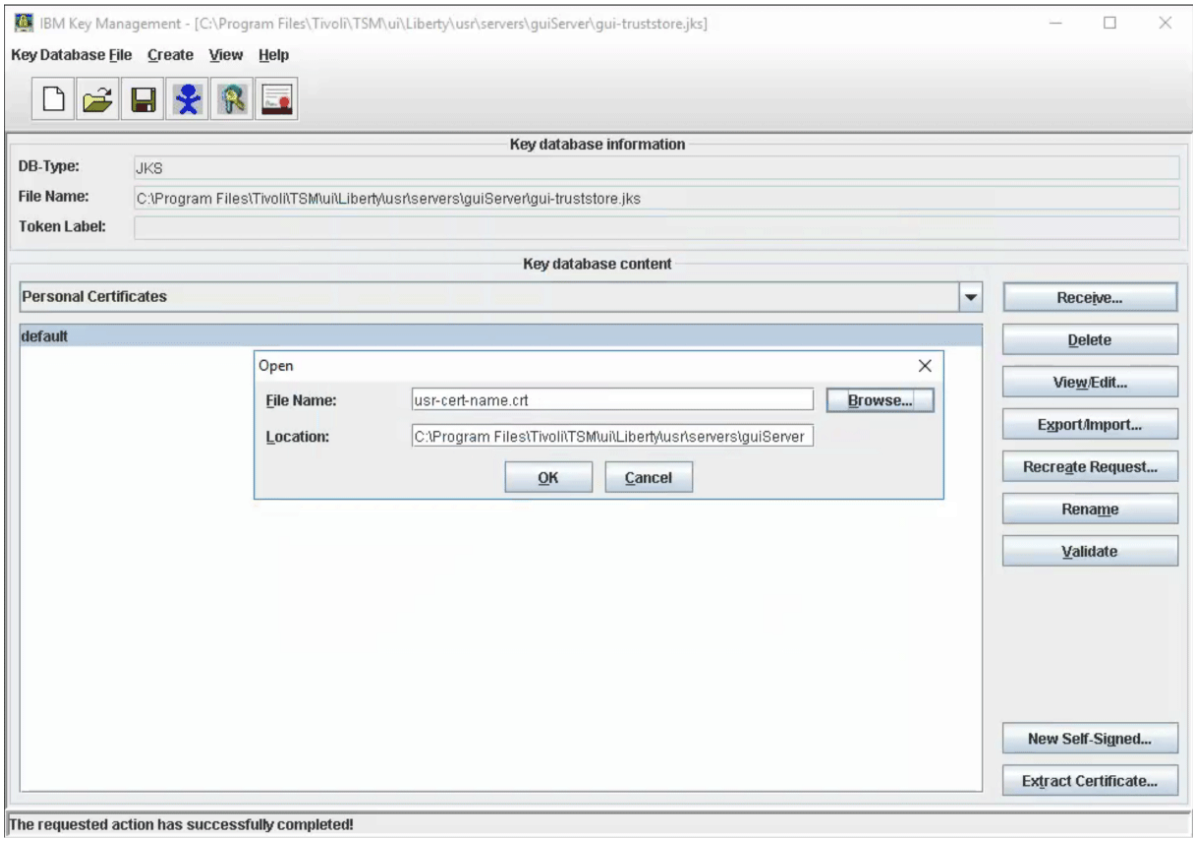


3. Получите подписанный сертификат, выполнив следующие шаги:

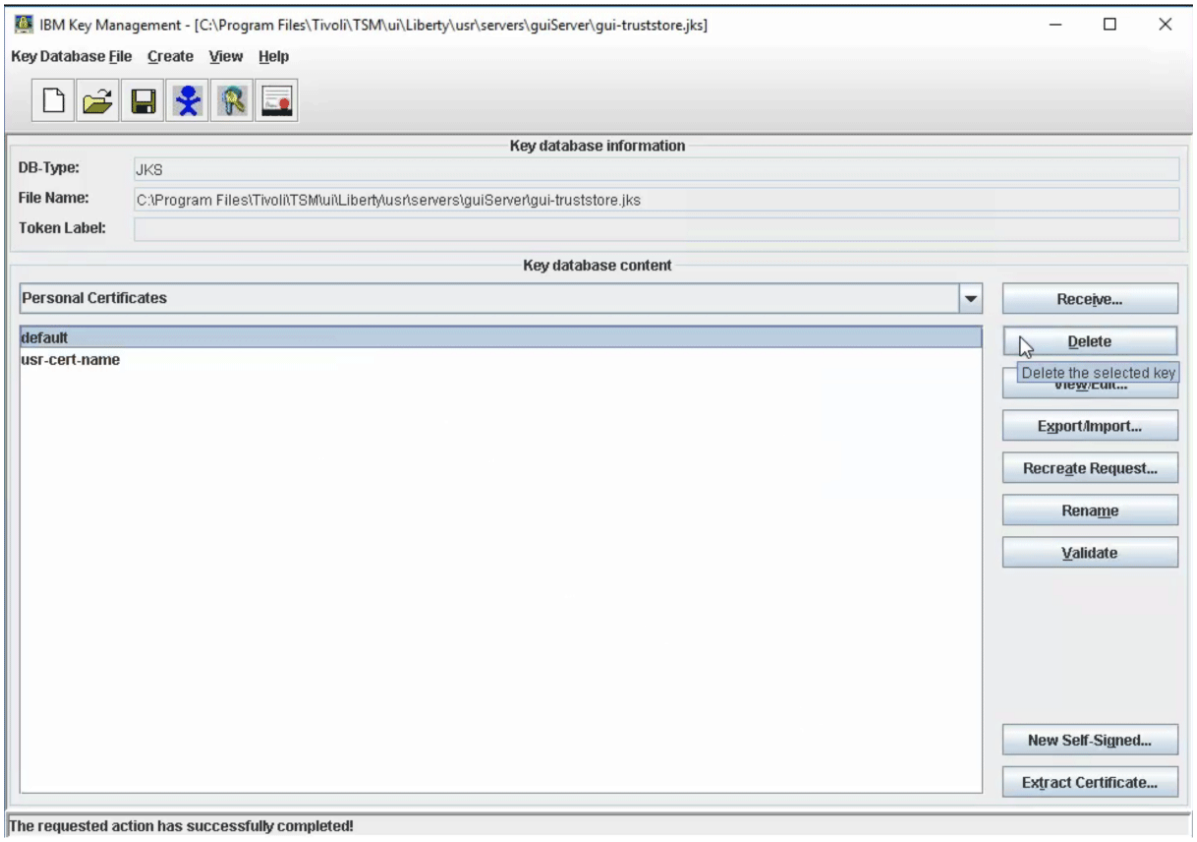
   a) В области **Содержимое базы данных ключей** выберите **Персональные сертификаты** и нажмите кнопку **Получить**.



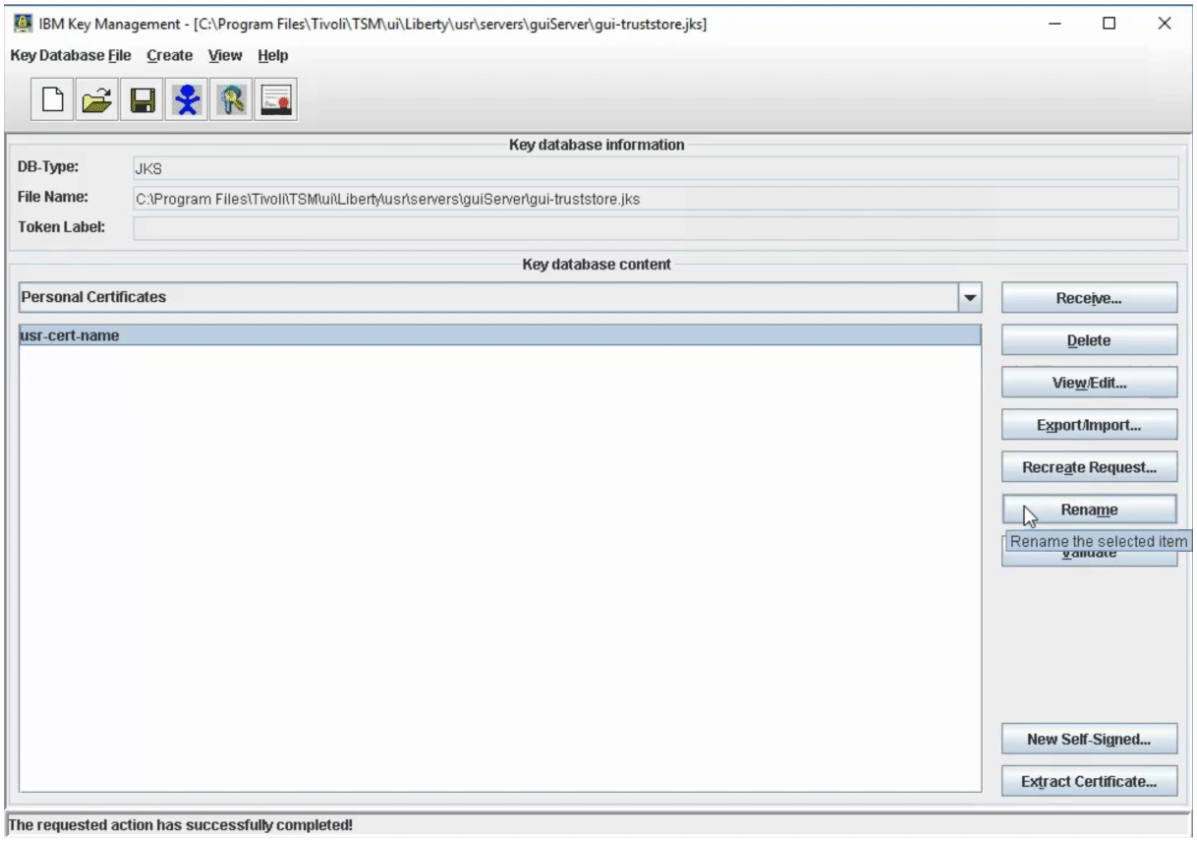
   b) В диалоговом окне Открыть укажите подписанный сертификат и нажмите кнопку **OK**.



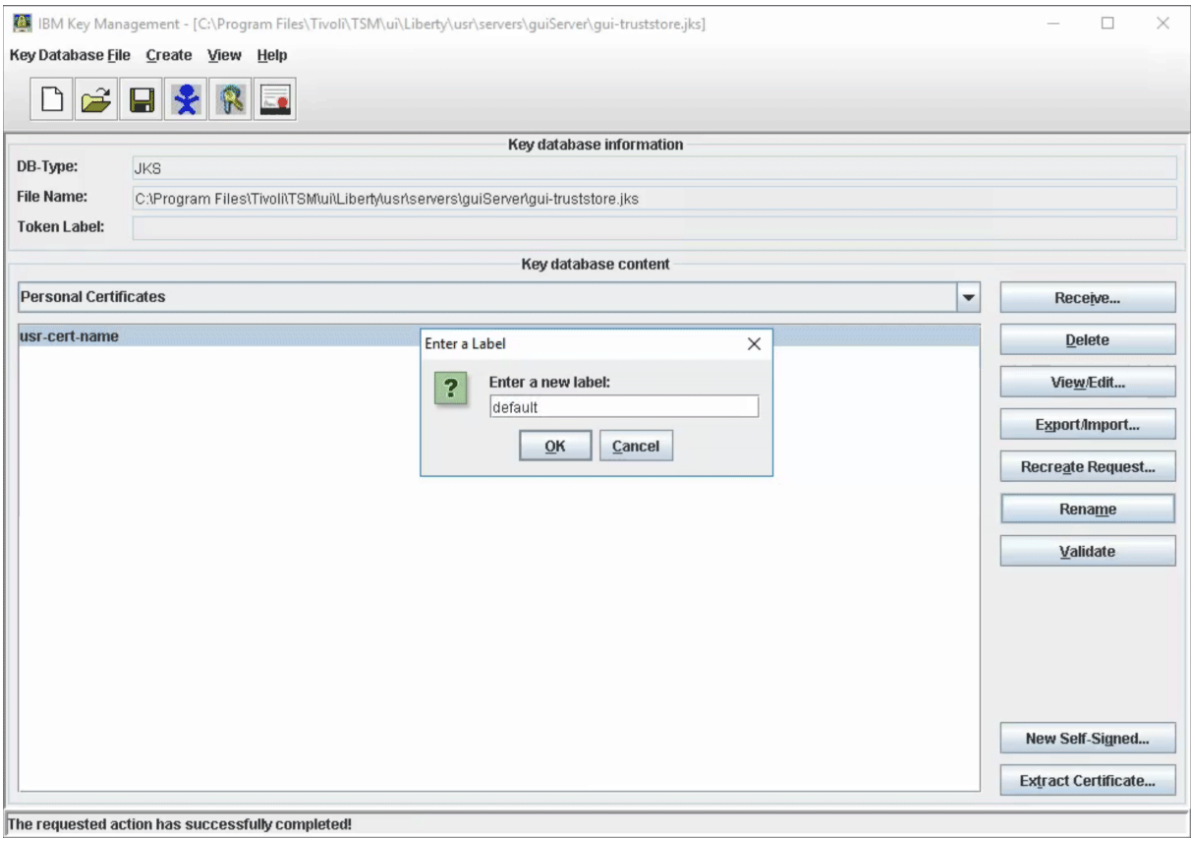
4. Удалите самоподписанный сертификат, который в настоящий момент используется компонентом Центр операций, и замените его на сертификат, подписанный сертификатором, выполнив следующие действия:
   a) В области **Содержимое базы данных ключей** выберите **Персональные сертификаты**.
   b) Выберите сертификат, помеченный **default** и нажмите кнопку **Удалить**. В диалоговом окне подтверждения нажмите кнопку **Да**.



c) Выберите подписанный центром сертификации сертификат **имя-сертификата-пользователя** и нажмите кнопку **Переименовать**.



d) В диалоговом окне Переименовать переименуйте подписанный сертификат (`имя-сертификата-пользователя`), задав для него имя `default`, и нажмите кнопку **ОК**.



5. Проверьте сертификат `default`, выполнив следующую команду:
   a) В области **Содержимое базы данных ключей** выберите **Персональные сертификаты**.
   b) Выберите сертификат, помеченный **default** и нажмите кнопку **Проверить**. В диалоговом окне подтверждения нажмите кнопку **OK**.
6. Запустите веб-сервер компонента Центр операций, как описано в разделе “Запуск и остановка веб-сервера” на стр. 184.

Получение подписанного сертификата при помощи команды `ikeycmd`

Если вы используете команду **`ikeycmd`**, которая открывает командную строку для управления ключами сертификатов и получения подписанных сертификатов.

Процедура

1. Убедитесь, что персональный подписанный сертификат находится в подходящем каталоге, введя команду **`ikeycmd`**. Выполните следующие шаги:
   a) Введите следующую команду:

   ```
   ikeycmd -certreq -list -db gui-truststore.jks
   ```

   Совет: Возможно, вам потребуется указать полный путь к команде **`ikeycmd`**. Команды расположены в следующем каталоге, где *каталог_установки* представляет каталог, в который устанавливается Центр операций:

   каталог_установки`/ui/jre/bin`

   b) В сообщении выводится имя персонального подписанного сертификата `имя-сертификата-пользователя`, находящегося в файле склада доверенных сертификатов.
2. Добавьте в файл склада доверенных сертификатов корневой сертификат CA и все промежуточные сертификаты, используя следующие команды. Если вы получили промежуточные сертификаты от CA, перед добавлением корневого сертификата CA нужно добавить их в файл склада доверенных сертификатов.

```
ikeycmd -cert -add -db gui-truststore.jks
    -file файл_промежуточного_сертификата
```

```
ikeycmd -cert -add -db gui-truststore.jks
    -file файл_корневого_сертификата
```

Здесь используются следующие обозначения:

-file *файл_сертификата*
Задает имя файла, в котором содержится сертификат.

3. Получите подписанный сертификат, введя следующую команду:

```
ikeycmd -cert -receive -db gui-truststore.jks
-file файл_сертификата_подписавшего
```

Здесь используются следующие обозначения:

-file *файл_сертификата_подписавшего*
Задает имя файла, в котором содержится подписанный сертификат.

4. Удалите самоподписанный сертификат, который в настоящий момент используется компонентом Центр операций, и замените его на сертификат, подписанный сертификатором, выполнив следующие действия:
   a) Чтобы удалить существующий самоподписанный сертификат, введите следующую команду:

```
ikeycmd -cert -delete -db gui-truststore.jks -label default
```

   b) Чтобы переименовать подписанный центром сертификации сертификат из *имя-сертификата-пользователя* в `default`, введите следующую команду:

```
ikeycmd -cert -rename -db gui-truststore.jks -label имя-сертификата-пользователя
-new_label default
```

Здесь используются следующие обозначения:

-label *имя-сертификата-пользователя*
Указывает сертификат, подписанный сертификатором, по его метке.

5. Проверьте сертификат `default`, введя следующую команду:

```
ikeycmd -cert -validate -db gui-truststore.jks -label default
```

6. Запустите веб-сервер Центра операций выполнив инструкции в разделе “Запуск и остановка веб-сервера” на стр. 184.

Удаление и переназначение пароля файла склада доверенных сертификатов Центра операций

Чтобы настроить защищенную связь между компонентом Центр операций и хаб-сервером, вы должны знать пароль файла склада доверенных сертификатов компонента Центр операций. Этот пароль создается при установке компонента Центр операций. Если вы не знаете пароль, можно удалить и переназначить его.

Об этой задаче

Чтобы назначить новый пароль, нужно создать пароль, удалить файл склада доверенных сертификатов компонента Центр операций и перезапустить веб-сервер компонента Центр операций.

Внимание:

Если вы забыли пароль склада доверенных сертификатов, надо получить новый подписанный сертификат от центра сертификации. Дополнительную информацию смотрите в разделе “Получение подписанного сертификата” на стр. 174.

Выполняйте эти шаги, только если вам неизвестен пароль склада доверенных сертификатов. Не выполняйте эти шаги, если вам известен пароль склада доверенных сертификатов и вы хотите изменить его. Чтобы удалить и переназначить пароль, нужно удалить файл склада доверенных сертификатов; при этом будут удалены все сертификаты, которые хранятся в файле склада доверенных сертификатов. Если вам известен пароль склада доверенных сертификатов, можно изменить его, используя **ikeycmd** или утилиту **ikeyman**.

Процедура

1. Остановите веб-сервер Центра операций
2. Перейдите в следующий каталог, где *каталог_установки* - это каталог, в котором установлен Центр операций:

   каталог_установки/ui/Liberty/usr/servers/guiServer
3. Откройте файл bootstrap.properties, содержащий пароль файла склада доверенных сертификатов.

   Если пароль не зашифрован, вы можете открыть с его помощью файла склада доверенных сертификатов, не переназначая пароль.

   В следующих примерах показана разница между зашифрованным и незашифрованным паролями:

   Пример зашифрованного пароля
   Зашифрованные пароли начинаются со строки {xor}.

   В следующем примере показан зашифрованный пароль в качестве значения параметра **tsm.truststore.pswd**:

   ```
   tsm.truststore.pswd={xor}MiYPPiwsKDAtOw==
   ```

   Пример незашифрованного пароля
   В следующем примере показан незашифрованный пароль в качестве значения параметра **tsm.truststore.pswd**:

   ```
   tsm.truststore.pswd=J8b%^B
   ```
4. Замените пароль в файле bootstrap.properties на новый пароль.

   Пароль можно заменить на зашифрованный или на незашифрованный пароль. Запомните незашифрованный пароль для последующего использования.

   Чтобы создать зашифрованный пароль, сделайте следующее:

   a. Создайте незашифрованный пароль.

      Пароль для склада доверенных сертификатов должен отвечать следующим критериям:

      - Пароль должен содержать не менее 6 и не более 64 символов.
      - Пароль должен содержать, как минимум, следующие символы:
        - Одну заглавную букву (A – Z)
        - Одну строчную букву (a – z)
        - Одну цифру (0 – 9)
        - Два символа, не являющихся алфавитно-цифровыми, которые указаны в следующем ряду:

          ```
          ~ @ # $ % ^ & * _ - + = ` |
          ```

          ```
          ( ) { } [ ] : ; < > , . ? /
          ```

   b. В командной строке операционной системы перейдите в следующий каталог:

каталог_установки/ui/Liberty/bin

c. Чтобы зашифровать пароль, введите следующую команду, где *пароль* - это незашифрованный пароль:

securityUtility encode *пароль* --encoding=aes

5. Сохраните файл bootstrap.properties.
6. Перейдите в следующий каталог:

каталог_установки/ui/Liberty/usr/servers/guiServer

7. Удалите файл gui-truststore.jks, который является файлом склада доверенных сертификатов компонента Центр операций.
8. Запустите веб-сервер компонента Центр операций.

Информацию о запуске веб-сервера компонента Центр операций смотрите в разделе “Запуск и остановка веб-сервера” на стр. 184.

Результаты

Новый файл склада доверенных сертификатов создается автоматически для компонента Центр операций, и сертификат TLS компонента Центр операций автоматически включается в файл склада доверенных сертификатов.

Запуск и остановка веб-сервера

Веб-сервер Центра операций работает как служба и запускается автоматически. Вам может потребоваться остановить и повторно запустить Web-сервер, например, чтобы произвести изменения конфигурации.

Процедура

Остановите и перезапустите Web-сервер.

- Если в системе установлен **systemctl**, введите следующие команды:
  - Чтобы остановить сервер:

```
systemctl stop opscenter.service
```

  - Чтобы запустить сервер:

```
systemctl start opscenter.service
```

  - Чтобы перезапустить сервер:

```
systemctl restart opscenter.service
```

  - Чтобы определить, работает ли сервер, введите следующую команду:

```
systemctl status opscenter.service
```

- Если **systemctl** не установлен в системе, введите следующие команды:
  - Чтобы остановить сервер:

```
service opscenter.rc stop
```

  - Чтобы запустить сервер:

```
service opscenter.rc start
```

  - Чтобы перезапустить сервер:

```
service opscenter.rc restart
```

– Для определения, запущен ли сервер, введите следующую команду:

```
service opscenter.rc status
```

Открытие Центра операций

Страница **Обзор** - это начальное представление по умолчанию в Центре операций. Однако в веб-браузере можно поместить в закладки страницу, которую вы хотите открывать при входе в Центр операций.

Процедура

1. В браузере введите следующий адрес, где *имя_хоста* - это имя компьютера, на котором установлен Центр операций, а *защищенный_порт* - это номер порта, который Центр операций использует для связи HTTPS на этом компьютере:

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

   Советы:

   - В URL учитывается регистр символов. Например, убедитесь, что вы ввели "oc" строчными буквами, как это показано.
   - Номер порта по умолчанию для связи HTTPS - 11090, но другой номер порта в диапазоне 1024 - 65535 можно указать при установке Центра операций. После установки администратор может сконфигурировать Центр операций для использования стандартного защищенного порта TCP/IP (порт 443) для связи HTTPS. Если Центр операций сконфигурирован для использования порта 443, то при открытии Центра операций не нужно включать номер защищенного порта. Вместо этого можно ввести следующий адрес, где *имя_хоста* - это имя компьютера, на котором установлен Центр операций:

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

     Дополнительную информацию о конфигурировании Центра операций для использования порта 443 смотрите в разделе “Конфигурирование веб-сервера Центра операций для использования стандартного защищенного порта TCP/IP” на стр. 162.
2. Войдите в систему с ID администратора, который зарегистрирован на хаб-сервере.

   На странице **Обзор** показана сводная информация для клиентов, служб, серверов, пулов хранения и устройств хранения. Чтобы просмотреть дополнительные сведения, можно щелкнуть по этим элементам или использовать панель меню Центра операций.

   Отслеживание с мобильного устройства: Чтобы удаленно отслеживать среду хранения, можно просматривать страницу **Обзор** Центра операций в веб-браузере мобильного устройства. Центр операций поддерживает веб-браузер Apple Safari на iPad. Можно использовать и другие мобильные устройства.

Сбор диагностической информации посредством службы управления клиентом Tivoli Storage Manager

служба управления клиентами собирает диагностическую информацию о клиентах резервного копирования и архивирования и делает ее доступной для Центра операций для основных функций мониторинга.

Об этой задаче

После установки службы управления клиентом на странице **Диагностика** в Центре операций содержится диагностическая информация для клиентов резервного копирования и архивирования.

Совет: Перед установкой служба управления клиентами убедитесь, что между клиентом резервного копирования-архивирования и сервером успешно установлено соединение. В файле склада доверенных сертификатов сервера, используемого клиентом, не будет сертификата Secure Sockets Layer (SSL) сервера, пока система клиента не соединится с сервером.

Диагностическую информацию можно собрать только с клиентов Linux и Windows, но администраторы могут просматривать диагностическую информацию по компоненту Центр операций в операционных системах AIX, Linux или Windows.

Также можно установить компонент служба управления клиентами на узлах перемещения данных для IBM Spectrum Protect for Virtual Environments: Data Protection for VMware, чтобы собирать диагностическую информацию о функциях перемещения данных.

Совет: В документации к службе управления клиентом *компьютер клиента* - это компьютер, на котором установлен клиент резервного копирования и архивирования.

Установка службы управления клиентом при помощи графического мастера

Для сбора диагностической информации о клиентах резервного копирования и архивирования (например, файлов журналов клиентов) нужно установить службу управления клиентом на управляемых компьютерах клиентов.

Прежде чем начать

Ознакомьтесь с разделом “Требования и ограничения для службы управления клиентом” на стр. 143.

Об этой задаче

Службу управления клиентом нужно установить на компьютере, на котором установлен клиент резервного копирования и архивирования.

Процедура

1. Скачайте пакет установки компонента служба управления клиентами с такого сайта скачивания IBM, как IBM Passport Advantage или IBM Fix Central. Ищите имя файла, аналогичное следующему: `<версия>-IBM-SPCMS-<операционная система>.bin`.

   В следующей таблице приведены имена пакетов установки.

Операционная система клиента	Имя пакета установки
Linux x86 64-битная	`8.1.x.000-IBM-SPCMS-Linuxx64.bin`
Windows 32-битная	`8.1.x.000-IBM-SPCMS-Windows32.exe`
Windows 64-битная	`8.1.x.000-IBM-SPCMS-Windows64.exe`

2. Создайте каталог на компьютере клиента, которым вы хотите управлять, и скопируйте в него пакет установки.
3. Распакуйте контент файла пакета установки.
   - На компьютерах клиента Linux сделайте следующее:
     a. Преобразуйте файл в выполняемый файл; для этого введите следующую команду:

     ```
     chmod +x 8.1.x.000-IBM-SPCMS-Linuxx64.bin
     ```

     b. Введите следующую команду:

     ```
     ./8.1.x.000-IBM-SPCMS-Linuxx64.bin
     ```

- На компьютерах клиента Windows дважды щелкните по имени пакета установки в Проводнике Windows.

Совет: Если вы ранее установили и деинсталлировали пакет, то выберите **Все**, когда вам предложат заменить существующие файлы установки.

4. Запустите пакетный файл установки из каталога, в который вы распаковали файлы установки и связанные файлы. Это каталог, который вы создали на шаге “2” на стр. 186.
   - На компьютерах клиента Linux введите следующую команду:

     ```
     ./install.sh
     ```

   - На компьютерах клиента Windows дважды щелкните по **install.bat**.
5. Для установки службы управления клиентом выполните инструкции в мастере IBM Installation Manager.

   Если продукт IBM Installation Manager не установлен на компьютере клиента, нужно выбрать и **IBM Installation Manager**, и **Службы управления клиентом IBM Spectrum Protect**.

   Совет: Можно принять значения по умолчанию для каталога общих ресурсов и каталога установки IBM Installation Manager.

Дальнейшие действия

Проверьте установку.

Установка компонента служба управления клиентами в режиме без вывода сообщений

Службу управления клиентом можно установить в режиме без вывода сообщений. В режиме без вывода сообщений вы задаете значения установки в файле ответов, а затем запускаете команду установки.

Прежде чем начать

Ознакомьтесь с разделом “Требования и ограничения для службы управления клиентом” на стр. 143.

Распакуйте пакет установки, выполнив инструкции в разделе “Установка службы управления клиентом при помощи графического мастера” на стр. 186.

Об этой задаче

Службу управления клиентом нужно установить на компьютере, на котором установлен клиент резервного копирования и архивирования.

Каталог `input`, находящийся в каталоге, в который извлечен пакет установки, содержит следующий пример файла ответов:

`install_response_sample.xml`

Вы можете использовать пример файла со значениями по умолчанию или настроить его.

Совет: Чтобы настроить пример файла, создайте копию примера файла, переименуйте ее и измените копию.

Процедура

1. Создайте файл ответов на основе файла примера или используйте пример файла ответов `install_response_sample.xml`.

В любом случае убедитесь, что в файле ответов указан номер порта для службы управления клиентом. Порт по умолчанию - 9028. Например:

```
<variable name='port' value='9028'/>
```

2. Введите команду установки службы управления клиентом и примите лицензию. В каталоге, в который извлечен файл установочного пакета, введите следующую команду, где *файл_ответов* - это полное имя файла ответов:

   На компьютере клиента Linux:

   ```
   ./install.sh -s -input файл_ответов
   -acceptLicense
   ```

   Например:

   ```
   ./install.sh -s -input /cms_install/input/install_response.xml -acceptLicense
   ```

   На компьютере клиента Windows:

   ```
   install.bat -s -input файл_ответов -acceptLicense
   ```

   Например:

   ```
   install.bat -s -input c:\cms_install\input\install_response.xml -acceptLicense
   ```

Дальнейшие действия

Проверьте установку.

Проверка правильности установки службы управления клиентом

Чтобы можно было использовать службу управления клиентом для сбора диагностической информации о клиенте резервного копирования и архивирования, нужно убедиться, что служба правильно установлена и сконфигурирована.

Процедура

Введите на компьютере клиента в командной строке следующие команды, чтобы посмотреть конфигурацию службы управления клиентом:

- На компьютерах клиента Linux введите следующую команду:

  ```
  каталог_установки_клиента/cms/bin/CmsConfig.sh
  list
  ```

  где *каталог_установки_клиента* - это каталог установки клиента резервного копирования и архивирования. Например, если используется установка клиента по умолчанию, то введите следующую команду:

  ```
  /opt/tivoli/tsm/cms/bin/CmsConfig.sh list
  ```

  Результат выполнения команды выглядит примерно так:

  ```
  Список конфигурации CMS

  server1.example.com:1500 NO_SSL HOSTNAME
  Возможности: [LOG_QUERY]
      Путь опций: /opt/tivoli/tsm/client/ba/bin/dsm.sys

      Файл журнала: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252

      Файл журнала: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252
  ```

- На компьютерах клиента Windows введите следующую команду:

```
каталог_установки_клиента\cms\bin\CmsConfig.bat list
```

где *каталог_установки_клиента* - это каталог установки клиента резервного копирования и архивирования. Например, если используется установка клиента по умолчанию, то введите следующую команду:

```
C:\"Program Files"\Tivoli\TSM\cms\bin\CmsConfig.bat list
```

Результат выполнения команды выглядит примерно так:

```
Список конфигурации CMS

server1.example.com:1500 NO_SSL HOSTNAME
Возможности: [LOG_QUERY]
    Путь опций: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

    Файл журнала: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252

    Файл журнала: C:\Program Files\Tivoli\TSM\baclient\dsmsched.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

Если служба управления клиентами правильно установлена и сконфигурирована, то в выходных результатах показан каталог файла журнала ошибок.

Выходной текст извлекается из следующего файла конфигурации:

- На компьютерах клиента Linux:

```
каталог_установки_клиента/cms/Liberty/usr/servers/cmsServer/client-configuration.xml
```

- На компьютерах клиента Windows:

```
каталог_установки_клиента\cms\Liberty\usr\servers\cmsServer\client-configuration.xml
```

Если в выходных результатах нет ни одной записи, то нужно сконфигурировать файл `client-configuration.xml`. Инструкции по конфигурированию этого файла смотрите в разделе Конфигурирование службы управления клиентами для пользовательских конфигураций. Можно использовать команду **CmsConfig verify**, чтобы проверить, правильно ли создано определение узла в файле `client-configuration.xml`.

Конфигурирование Центра операций для использования службы управления клиентом

Если вы не использовали для службы управления клиентом конфигурацию по умолчанию, то нужно сконфигурировать Центр операций для доступа к службе управления клиентом.

Прежде чем начать

Убедитесь, что служба управления клиентами установлена и запущена на компьютере клиента. Ознакомьтесь с разделом “Требования и ограничения для службы управления клиентом” на стр. 143.

Проверьте, используется ли конфигурация по умолчанию. Конфигурация по умолчанию не используется в следующих случаях:

- Служба управления клиентом не использует номер порта по умолчанию (9028).
- Для клиента резервного копирования и архивирования не используется IP-адрес, который используется для компьютера клиента резервного копирования и архивирования. Например, другой IP-адрес может использоваться в следующих случаях:

– В компьютерной системе установлено две сетевые карты. Клиент резервного копирования и архивирования сконфигурирован для взаимодействия с одной сетью, а служба управления клиентами взаимодействует с другой сетью.
– На компьютере клиента используется DHCP. Поэтому компьютеру клиента динамически назначается IP-адрес, сохраненный на сервере IBM Spectrum Protect во время предыдущей операции клиента резервного копирования и архивирования. При перезагрузке компьютера клиента ему может быть назначен другой IP-адрес. Чтобы Центр операций всегда мог найти компьютер клиента, нужно задать полное имя домена.

Процедура

Чтобы сконфигурировать Центр операций для использования службы управления клиентом, сделайте следующее:

1. Выберите клиента на странице **Клиенты** Центра операций.
2. Щелкните по **Сведения**.
3. Щелкните по вкладке **Свойства**.
4. В поле **URL удаленной диагностики** раздела **Общее** укажите URL для службы управления клиентом на компьютере клиента.

   Адрес должен начинаться с `https`. В следующей таблице показаны примеры URL удаленной диагностики.

Тип URL	Пример
С именем хоста DNS и портом по умолчанию (9028)	`https://server.example.com`
С именем хоста DNS и портом не по умолчанию	`https://server.example.com:1599`
С IP-адресом и портом не по умолчанию	`https://192.0.2.0:1599`

5. Нажмите кнопку **Сохранить**.

Дальнейшие действия

Вы можете получить доступ к диагностической информации о клиенте (например, к файлам журнала клиента) на вкладке **Диагностика** в Центре операций.

Запуск и остановка компонента служба управления клиентами

Служба управления клиентом автоматически запускается после установки службы на компьютере клиента. В некоторых случаях может понадобиться остановить и запустить службу.

Процедура

- Чтобы остановить, запустить или перезапустить службу управления клиентом на компьютерах клиента Linux, введите следующую команду:
  - Если в системе установлен **systemctl**, введите следующие команды:
    - Чтобы остановить сервер:

      ```
      systemctl stop cms.service
      ```

    - Чтобы запустить сервер:

      ```
      systemctl start cms.service
      ```

    - Чтобы перезапустить сервер:

      ```
      systemctl restart cms.service
      ```

- Для определения, запущен ли сервер, введите следующую команду:

```
systemctl status cms.service
```

- Если **systemctl** не установлен в системе, введите следующие команды:
  - Чтобы остановить сервер:

```
service cms.rc stop
```

  - Чтобы запустить сервер:

```
service cms.rc start
```

  - Чтобы перезапустить сервер:

```
service cms.rc restart
```

  - Для определения, запущен ли сервер, введите следующую команду:

```
service cms.rc status
```

- На компьютерах клиента Windows откройте окно **Службы** и остановите, запустите или перезапустите службу IBM Spectrum Protect Client Management Services.

Удаление компонента служба управления клиентами

Если вам больше не нужно собирать диагностическую информацию о клиенте, то вы можете деинсталлировать службу управления клиентом с компьютера клиента.

Об этой задаче

Для деинсталляции службы управления клиентом нужно использовать IBM Installation Manager. Если вы больше не собираетесь использовать IBM Installation Manager, то его также можно деинсталлировать.

Процедура

1. Деинсталлируйте службу управления клиентом с компьютера клиента:
   a) Откройте IBM Installation Manager:
      - На компьютере клиента Linux перейдите в каталоге установки IBM Installation Manager в подкаталог `eclipse` (например, `/opt/IBM/InstallationManager/eclipse`) и введите следующую команду:

```
./IBMIM
```

      - На компьютере клиента Windows откройте IBM Installation Manager из меню **Пуск**.
   b) Щелкните по **Деинсталлировать**.
   c) Выберите **Службы управления клиентом IBM Spectrum Protect** и нажмите кнопку **Далее**.
   d) Щелкните по **Деинсталлировать** и щелкните по **Готово**.
   e) Закройте окно **IBM Installation Manager**.
2. Если IBM Installation Manager больше не нужен, то деинсталлируйте его с компьютера клиента:
   a) Откройте мастер деинсталляции IBM Installation Manager:
      - На компьютере клиента Linux перейдите в каталог uninstall IBM Installation Manager (например, `/var/ibm/InstallationManager/uninstall`) и введите следующую команду:

```
./uninstall
```

- На компьютере клиента Windows щелкните по **Пуск** > **Панель управления**. После этого щелкните по **Деинсталляция программ** > **IBM Installation Manager** > **Деинсталлировать**.

b) В окне **IBM Installation Manager** выберите **IBM Installation Manager** и нажмите кнопку **Далее**.

c) Щелкните по **Деинсталлировать** и щелкните по **Готово**.

Конфигурирование службы управления клиентом для пользовательских установок клиента

Служба управления клиентом использует информацию в файле конфигурации клиента (`client-configuration.xml`) для обнаружения диагностической информации. Если служба управления клиентами не может обнаружить положение файлов журнала, то нужно запустить утилиту **CmsConfig**, чтобы добавить каталог файлов журнала в файл `client-configuration.xml`.

Об этой задаче

Перед установкой служба управления клиентами убедитесь, что между клиентом резервного копирования-архивирования и сервером успешно установлено соединение. В файле склада доверенных сертификатов сервера, используемого клиентом, не будет сертификата Secure Sockets Layer (SSL) сервера, пока система клиента не соединится с сервером.

Утилита CmsConfig

Если вы не используете конфигурацию клиента по умолчанию, вы можете запустить на компьютере клиента утилиту **CmsConfig**, чтобы обнаружить каталог файлов журнала и добавить его в файл `client-configuration.xml`. После завершения конфигурирования служба управления клиентами сможет обращаться к файлам журнала клиента и делать их доступными для базовых диагностических функций в компоненте Центр операций.

При помощи утилиты **CmsConfig** можно также посмотреть конфигурацию службы управления клиентом и удалить имя узла из файла `client-configuration.xml`.

Файл `client-configuration.xml` находится в следующих каталогах:

- На компьютерах клиента Linux:

```
каталог_установки_клиента/cms/Liberty/usr/servers/cmsServer
```

- На компьютерах клиента Windows:

```
каталог_установки_клиента\cms\Liberty\usr\servers\cmsServer
```

где *каталог_установки_клиента* - это каталог установки клиента резервного копирования и архивирования.

Утилита **CmsConfig** расположена в следующих каталогах.

Операционная система клиента	Каталог и имя утилиты
Linux	*каталог_установки_клиента*/cms/bin/CmsConfig.sh
Windows	*каталог_установки_клиента*\cms\bin\CmsConfig.bat

Для использования утилиты **CmsConfig** введите любую команду, включенную в утилиту. Вводите команды в одной строке.

Команда CmsConfig discover

При помощи команды **CmsConfig discover** можно автоматически обнаружить файлы опций и журналов и добавить их в файл конфигурации клиента `client-configuration.xml`. После этого

служба управления клиентами сможет обращаться к файлам журнала клиента и делать их доступными для диагностики в компоненте Центр операций.

Обычно установщик службы управления клиентом автоматически запускает команду **CmsConfig discover**. Однако эту команду нужно запустить вручную, если вы изменили клиент резервного копирования и архивирования (например, добавили клиента или изменили конфигурацию сервера или каталог файлов журнала).

Чтобы служба управления клиентами могла создать определение журнала в файле `client-configuration.xml`, нужно получить адрес сервера IBM Spectrum Protect, порт сервера и имя клиентского узла. Если имя узла не задано в файле опций клиента (обычно `dsm.sys` в клиентах Linux и `dsm.opt` в клиентах Windows), то используется имя хоста компьютера клиента.

Для изменения файла конфигурации клиента служба управления клиентами должна иметь доступ к одному или нескольким файлам журнала (например, `dsmerror.log` и `dsmsched.log`). Для получения оптимальных результатов запускайте команду **CmsConfig discover** в каталоге, в котором вы запускаете команду **dsmc** клиента резервного копирования и архивирования, и с использованием тех же переменных среды. Таким образом вы можете повысить вероятность того, что будут найдены правильные файлы журнала.

Если файл опций клиента находится в пользовательском расположении или если у него нет типичного имени файла опций, вы также можете задать путь файла опций клиента, чтобы сузить область обнаружения.

Синтаксис

Параметры

configPath

Путь файла опций клиента (как правило, `dsm.opt`). Задайте путь конфигурации, если файл опций клиента не находится в расположении по умолчанию или если у него нет имени по умолчанию. служба управления клиентами загрузит файл опций клиента и на его основе обнаружит узлы и журналы клиента. Это необязательный параметр.

В системе клиента Linux служба управления клиентами всегда сначала загружает файл пользовательских опций клиента (`dsm.opt`), а затем ищет файл системных опций клиента (как правило, `dsm.sys`). Однако значение параметра *configPath* всегда является файлом пользовательских опций клиента.

Примеры для клиента Linux

- Обнаружить файлы журнала клиента и автоматически добавить определения журналов в файл `client-configuration.xml`.

  Введите из каталога `/opt/tivoli/tsm/cms/bin` следующую команду:

  Команда:

  ```
  ./CmsConfig.sh discover
  ```

  Выходные результаты:

  ```
  Обнаружение конфигурации и журналов клиента.

  server.example.com:1500 SUSAN
      /opt/tivoli/tsm/client/ba/bin/dsmerror.log

  Обнаружение конфигурации и журналов клиента завершено.
  ```

- Произведите обнаружение файлов конфигурации и файлов журналов, заданных в файле /opt/tivoli/tsm/client/ba/bin/daily.opt, и автоматически добавьте определения журналов в файл client-configuration.xml.

  Введите из каталога /opt/tivoli/tsm/cms/bin следующую команду:

  Команда:
  ```
  ./CmsConfig.sh discover /opt/tivoli/tsm/client/ba/bin/daily.opt
  ```

  Выходные результаты:

  ```
  Обнаружение конфигурации и журналов клиента

  server.example.com:1500 NO_SSL SUSAN
  Возможности: [LOG_QUERY]
      Путь опций: /opt/tivoli/tsm/client/ba/bin/dsm.sys

      Файл журнала: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252

      Файл журнала: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252

  Обнаружение конфигурации и журналов клиента завершено.
  ```

Примеры для клиента Windows

- Обнаружить файлы журнала клиента и автоматически добавить определения журналов в файл client-configuration.xml.

  Введите указанную ниже команду из каталога C:\Program Files\Tivoli\TSM\cms\bin:

  Команда:
  ```
  cmsconfig discover
  ```

  Выходные результаты:

  ```
  Обнаружение конфигурации и журналов клиента.

  server.example.com:1500 SUSAN
      C:\Program Files\Tivoli\TSM\baclient\dsmerror.log

  Обнаружение конфигурации и журналов клиента завершено.
  ```

- Произведите обнаружение файлов конфигурации и файлов журналов, заданных в файле c:\program files\tivoli\tsm\baclient\daily.opt, и автоматически добавьте определения журналов в файл client-configuration.xml.

  Введите указанную ниже команду из каталога C:\Program Files\Tivoli\TSM\cms\bin:

  Команда:
  ```
  cmsconfig discover "c:\program files\tivoli\tsm\baclient\daily.opt"
  ```

  Выходные результаты:

  ```
  Обнаружение конфигурации и журналов клиента

  server.example.com:1500 NO_SSL SUSAN
  Возможности: [LOG_QUERY]
      Путь опций: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

      Файл журнала: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252

      Файл журнала: C:\Program Files\Tivoli\TSM\baclient\dsmsched.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252

  Обнаружение конфигурации и журналов клиента завершено.
  ```

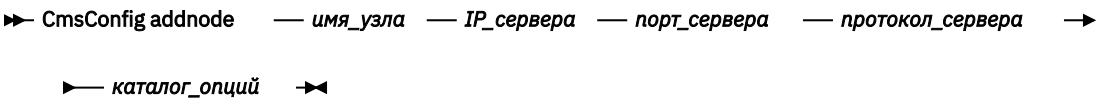
Команда CmsConfig addnode

Используйте команду **CmsConfig addnode**, чтобы вручную добавить определение клиентского узла в файл конфигурации client-configuration.xml. Определение узла содержит

информацию, необходимую компоненту служба управления клиентами для взаимодействия с сервером IBM Spectrum Protect.

Используйте эту команду, только если файл опций клиента или файлы журнала клиента хранятся на компьютере клиента не в каталоге по умолчанию.

Синтаксис



Параметры

имя_узла
Имя клиентского узла, связанное с файлами журнала. Для большинства систем клиентов на сервере IBM Spectrum Protect регистрируется только один узел. Однако в системах с несколькими пользователями (например, системы клиента Linux) может быть несколько клиентских узлов. Это обязательный параметр.

IP_сервера
Адрес TCP/IP сервера IBM Spectrum Protect, на котором аутентифицируется служба управления клиентами. Это обязательный параметр.

Адрес TCP/IP сервера может содержать от одного до 64 символов. Адрес сервера может быть именем домена TCP/IP или числовым IP-адресом. Числовой IP-адрес может быть адресом TCP/IP v4 или TCP/IP v6. Адреса IPv6 можно использовать, только если для компьютера клиента задана опция **commmethod V6Tcpip**.

Примеры:

- `server.example.com`
- `192.0.2.0`
- `2001:0DB8:0:0:0:0:0:0`

порт_сервера
Номер порта TCP/IP для связи с сервером IBM Spectrum Protect. Введите значение от 1 до 32767. Это обязательный параметр.

Пример: `1500`

протокол_сервера
Протокол, используемый для связи между службой управления клиентом и сервером IBM Spectrum Protect. Это обязательный параметр.

Возможны следующие значения.

Значение	Объяснение
NO_SSL	Протокол защиты SSL не используется.
SSL	Протокол защиты SSL используется.
FIPS	Протокол TLS 1.2 используется в режиме Federal Information Processing Standard (FIPS). **Совет:** Можно также ввести `TLS_1.2`, чтобы указать, что протокол используется в режиме FIPS.

каталог_опций
Полное имя каталога файла опций клиента. Это обязательный параметр.

Пример (клиент Linux): `/opt/backup_tools/tivoli/tsm/baclient/dsm.sys`

Пример (клиент Windows): `C:\backup tools\Tivoli\TSM\baclient\dsm.opt`

Пример для клиента Linux

Добавьте определение клиентского узла SUSAN в файл `client-configuration.xml`. Сервер IBM Spectrum Protect, с которым взаимодействует узел - это `server.example.com` на порту сервера 1500. Протокол защиты SSL не используется. Путь файла системных опций клиента - `/opt/tivoli/tsm/client/ba/bin/custom_opt.sys`.

Введите из каталога `/opt/tivoli/tsm/cms/bin` следующую команду:

Команда:

```
./CmsConfig.sh addnode SUSAN server.example.com 1500 NO_SSL /opt/tivoli/tsm/
client/ba/bin/custom_opt.sys
```

Выходные результаты:

```
Добавление узла.

Конфигурация клиента добавлена.
```

Пример для клиента Windows

Добавьте определение клиентского узла SUSAN в файл `client-configuration.xml`. Сервер IBM Spectrum Protect, с которым взаимодействует узел - это `server.example.com` на порту сервера 1500. Протокол защиты SSL не используется. Путь файла опций клиента - `c:\program files\tivoli\tsm\baclient\custom.opt`.

Введите следующую команду из каталога `C:\Program Files\Tivoli\TSM\cms\bin`:

Команда:

```
cmsconfig addnode SUSAN server.example.com 1500 NO_SSL "c:\program files
\tivoli\tsm\baclient\custom.opt"
```

Выходные результаты:

```
Добавление узла.

Конфигурация клиента добавлена.
```

Команда CmsConfig setopt

Используйте команду **CmsConfig setopt**, чтобы задать путь файла опций клиента (как правило, `dsm.opt`) в существующем определении узла, не читая сначала содержимое файла опций клиента.

Эта команда может оказаться полезной, если у файла опций клиента нет стандартного имени или если он находится не в расположении по умолчанию.

Требование: Если определение узла не существует, вы должны сначала ввести команду **CmsConfig addnode**, чтобы создать определение узла.

В отличие от команды **CmsConfig discover** команда **CmsConfig setopt** не создает связанные определения журналов в файле `client-configuration.xml`. Необходимо использовать команду **CmsComfog addlog** для создания определений журнала.

Синтаксис

Параметры

имя_узла

Имя клиентского узла, связанное с файлами журнала. Для большинства систем клиентов на сервере IBM Spectrum Protect регистрируется только один узел. Однако в системах с

несколькими пользователями (например, системы клиента Linux) может быть несколько клиентских узлов. Это обязательный параметр.

optPath
Полностью заданный путь файла опций клиента. Это обязательный параметр.

Пример (клиент Linux): `/opt/backup_tools/tivoli/tsm/baclient/dsm.opt`

Пример (клиент Windows): `C:\backup tools\Tivoli\TSM\baclient\dsm.opt`

Пример для клиента Linux

Задайте путь файла опций клиента для узла SUSAN. Путь файла опций клиента - `/opt/tivoli/tsm/client/ba/bin/dsm.opt`.

Введите из каталога `/opt/tivoli/tsm/cms/bin` следующую команду:

Команда:
```
./CmsConfig.sh setopt SUSAN /opt/tivoli/tsm/client/ba/bin/dsm.opt
```

Выходные результаты:

```
Добавление конфигурационного файла узла.

Завершено добавление файла конфигурации клиента.
```

Пример для клиента Windows

Задайте путь файла опций клиента для узла SUSAN. Путь файла опций клиента - `c:\program files\tivoli\tsm\baclient\dsm.opt`.

Введите указанную ниже команду из каталога `C:\Program Files\Tivoli\TSM\cms\bin`:

Команда:
```
cmsconfig setopt SUSAN "c:\program files\tivoli\tsm\baclient\dsm.opt"
```

Выходные результаты:

```
Добавление конфигурационного файла узла.

Завершено добавление файла конфигурации клиента.
```

Команда CmsConfig setsys

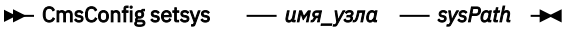
В случае системы клиента Linux используйте команду **CmsConfig setsys**, чтобы задать путь файла системных опций клиента (как правило, `dsm.sys`) в существующем определении узла, не читая сначала содержимое файла системных опций клиента.

Эта команда может оказаться полезной, если у файла системных опций клиента нет стандартного имени или если он находится не в расположении по умолчанию.

Требование: Если определение узла не существует, вы должны сначала ввести команду **CmsConfig addnode**, чтобы создать определение узла.

В отличие от команды **CmsConfig discover** команда **CmsConfig setsys** не создает связанные определения журналов в файле `client-configuration.xml`. Необходимо использовать команду **CmsComfog addlog** для создания определений журнала.

Синтаксис



Параметры

имя_узла
Имя клиентского узла, связанное с файлами журнала. Для большинства систем клиентов на сервере IBM Spectrum Protect регистрируется только один узел. Однако в системах с несколькими пользователями (например, системы клиента Linux) может быть несколько клиентских узлов. Это обязательный параметр.

sysPath
Полностью определенный путь клиентского файла системных опций. Это обязательный параметр.

Пример: `/opt/backup_tools/tivoli/tsm/baclient/dsm.sys`

Пример

Задайте путь файла системных опций клиента для узла SUSAN. Путь для клиентского файла системных опций: `/opt/tivoli/tsm/client/ba/bin/dsm.sys`.

Введите из каталога `/opt/tivoli/tsm/cms/bin` следующую команду:

Команда:

```
./CmsConfig.sh setopt SUSAN /opt/tivoli/tsm/client/ba/bin/dsm.sys
```

Выходные результаты:

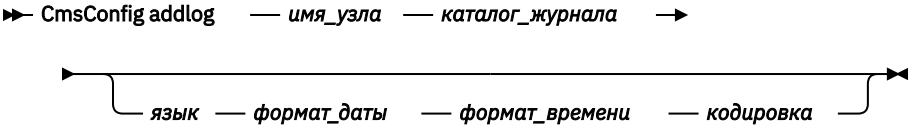
```
Добавление конфигурационного файла узла.
Завершено добавление файла конфигурации клиента.
```

Команда CmsConfig addlog

Используйте команду **CmsConfig addlog**, чтобы вручную добавить каталог файлов журналов клиента в существующее определение узла в файле конфигурации `client-configuration.xml`. Используйте эту команду, только если файлы журнала клиента хранятся на компьютере клиента не в каталоге по умолчанию.

Требование: Если определение узла не существует, вы должны сначала ввести команду **CmsConfig addnode**, чтобы создать определение узла.

Синтаксис



Параметры

имя_узла
Имя клиентского узла, связанное с файлами журнала. Для большинства систем клиентов на сервере IBM Spectrum Protect регистрируется только один узел. Однако в системах с несколькими пользователями (например, системы клиента Linux) может быть несколько клиентских узлов. Это обязательный параметр.

каталог_журнала
Полное имя каталога файлов журнала. Это обязательный параметр.

Пример (клиент Linux): `/opt/backup_tools/tivoli/tsm/baclient/dsmerror.log`

Пример (клиент Windows): `C:\backup tools\Tivoli\TSM\baclient\dsmerror.log`

язык
Локаль языка файла журнала. Это необязательный параметр. Однако если этот параметр задан, то нужно также задать параметры **формат_даты**, **формат_времени** и **кодировка**. Нужно задать локали для следующих языков:

Язык	Национальная версия
Бразильский португальский	pt_BR
Китайский упрощенный	zh_CN
Китайский традиционный	zh_TW
Чешский	cs_CZ
Английский	en_US
Французский	fr_FR
Немецкий	de_DE
Венгерский	hu_HU
Итальянский	it_IT
Японский	ja_JP
Корейский	ko_KR
Польский	pl_PL
Русский	ru_RU
Испанский	es_ES

формат_даты
Формат даты записей отметки времени в файле журнала клиента. Это необязательный параметр. Однако если этот параметр задан, то нужно также задать параметры **язык**, **формат_времени** и **кодировка**.

В следующей таблице перечислены форматы даты для языков.

Совет: Вместо того, чтобы использовать форматы дат, перечисленные в таблице, можно задать формат даты при помощи опции **dateformat** клиента резервного копирования и архивирования.

Язык	Формат даты
Китайский упрощенный	yyyy-MM-dd
Китайский традиционный	yyyy/MM/dd
Чешский	dd.MM.yyyy
Английский	dd.MM.yyyy
Французский	dd/MM/yyyy
Немецкий	dd.MM.yyyy
Венгерский	yyyy.MM.dd
Итальянский	dd/MM/yyyy
Японский	yyyy-MM-dd
Корейский	yyyy/MM/dd
Польский	yyyy-MM-dd

Язык	Формат даты
Бразильский португальский	dd/MM/yyyy
Русский	dd.MM.yyyy
Испанский	dd.MM.yyyy

формат_времени
Формат времени записей отметки времени в файле журнала клиента. Это необязательный параметр. Однако если этот параметр задан, то нужно также задать параметры **язык**, **формат_даты** и **кодировка**.

В следующей таблице приведены примеры форматов времени по умолчанию, которые можно указать для различных операционных систем клиента.

Совет: Вместо того, чтобы использовать форматы времени, перечисленные в таблице, можно задать формат времени при помощи опции **timeformat** клиента резервного копирования и архивирования.

Язык	Формат времени для клиентов Linux	Формат времени для клиентов Windows
Китайский упрощенный	HH:mm:ss	HH:mm:ss
Китайский традиционный	HH:mm:ss	ahh:mm:ss
Чешский	HH:mm:ss	HH:mm:ss
Английский	HH:mm:ss	HH:mm:ss
Французский	HH:mm:ss	HH:mm:ss
Немецкий	HH:mm:ss	HH:mm:ss
Венгерский	HH.mm.ss	HH:mm:ss
Итальянский	HH:mm:ss	HH:mm:ss
Японский	HH:mm:ss	HH:mm:ss
Корейский	HH:mm:ss	HH:mm:ss
Польский	HH:mm:ss	HH:mm:ss
Бразильский португальский	HH:mm:ss	HH:mm:ss
Русский	HH:mm:ss	HH:mm:ss
Испанский	HH:mm:ss	HH:mm:ss

кодировка
Кодировка символов записей в файле журнала клиента. Это необязательный параметр. Однако если этот параметр задан, то нужно также задать параметры **язык**, **формат_даты** и **формат_времени**.

Обычная кодировка для клиентов Linux - UTF-8. Для клиентов Windows значения кодировки по умолчанию приведены в следующей таблице. Если система клиента настроена иначе, то используйте параметр **кодировка**, чтобы задать значение не по умолчанию.

Язык	Кодировка
Китайский упрощенный	CP936
Китайский традиционный	CP950
Чешский	Windows-1250

Язык	Кодировка
Английский	Windows-1252
Французский	Windows-1252
Немецкий	Windows-1252
Венгерский	Windows-1250
Итальянский	Windows-1252
Японский	CP932
Корейский	CP949
Польский	Windows-1250
Бразильский португальский	Windows-1252
Русский	Windows-1251
Испанский	Windows-1252

Пример для клиента Linux

Добавьте расположение файла журнала клиента в существующее определение клиентского узла SUSAN в файле `client-configuration.xml`. Путь файла журнала клиента - `/usr/work/logs/dsmerror.log`. Добавьте спецификацию языка, формат времени и формат дат для французской локали.

Введите из каталога `/opt/tivoli/tsm/cms/bin` следующую команду:

Команда:

```
./CmsConfig.sh addlog SUSAN /usr/work/logs/dsmerror.log fr_FR yyyy/MM/dd
HH:MM:ss UTF-8
```

Выходные результаты:

```
Добавление журнала.

Завершено добавление журнала.
```

Пример для клиента Windows

Добавьте расположение файла журнала клиента в существующее определение клиентского узла SUSAN в файле `client-configuration.xml`. Путь файла журнала клиента - `c:\work\logs\dsmerror.log`. Добавьте спецификацию языка, формат времени и формат дат для французской локали.

Введите указанную ниже команду из каталога `C:\Program Files\Tivoli\TSM\cms\bin`:

Команда:

```
cmsconfig addlog SUSAN c:\work\logs\dsmerror.log fr_FR yyyy/MM/dd HH:MM:ss
UTF-8
```

Выходные результаты:

```
Добавление журнала.

Завершено добавление журнала.
```

Команда `CmsConfig remove`

Команда **`CmsConfig remove`** удаляет определение клиентского узла из файла конфигурации клиента `client-configuration.xml`. Удаляются также все записи в файле журнала, связанные с именем клиентского узла.

Синтаксис

Параметры

имя_узла
Имя клиентского узла, связанное с файлами журнала. Для большинства систем клиентов на сервере IBM Spectrum Protect регистрируется только один узел. Однако в системах с несколькими пользователями (например, системы клиента Linux) может быть несколько клиентских узлов. Это обязательный параметр.

Пример для клиента Linux

Удалить определение узла SUSAN из файла `client-configuration.xml`.

Введите из каталога `/opt/tivoli/tsm/cms/bin` следующую команду:

Команда:

```
./CmsConfig.sh remove SUSAN
```

Выходные результаты:

```
Удаление узла.

Удаление узла завершено.
```

Пример для клиента Windows

Удалить определение узла SUSAN из файла `client-configuration.xml`.

Введите указанную ниже команду из каталога `C:\Program Files\Tivoli\TSM\cms\bin`:

Команда:

```
cmsconfig remove SUSAN
```

Выходные результаты:

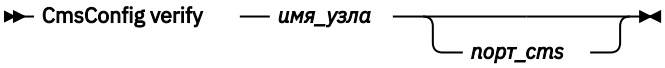
```
Удаление узла.

Удаление узла завершено.
```

Команда CmsConfig verify

Команда **CmsConfig verify** проверяет, правильно ли создано определение узла в файле `client-configuration.xml`. Если будут обнаружены ошибки, связанные с определением узла или если узел задан неправильно, вы должны исправить определение узла при помощи соответствующих команд **CmsConfig**.

Синтаксис



Параметры

имя_узла
Имя клиентского узла, связанное с файлами журнала. Для большинства систем клиентов на сервере IBM Spectrum Protect регистрируется только один узел. Однако в системах с несколькими пользователями (например, системы клиента Linux) может быть несколько клиентских узлов. Это обязательный параметр.

порт_cms
Номер порта TCP/IP для связи с служба управления клиентами. Если во время установки компонента служба управления клиентами вы не использовали номер порта по умолчанию, укажите номер порта. Номер порта по умолчанию - 9028. Это необязательный параметр.

Пример для клиента Linux

Убедиться, что определение узла SUSAN правильно создано в файле `client-configuration.xml`.

Введите из каталога `/opt/tivoli/tsm/cms/bin` следующую команду:

Команда:
```
./CmsConfig.sh verify SUSAN
```

Во время проверки вас попросят ввести имя клиентского узла или ID администратора и пароль.

Выходные результаты:

```
Проверка узла.


Проверка конфигурации службы CMS для узла SUSAN.
Конфигурация CMS правильная.

Проверка правильности работы службы CMS на порту 9028.

Введите ваш ID пользователя: admin
Введите ваш пароль:

Устанавливается соединение со службой CMS и проверяются ресурсы.
Служба CMS работает правильно.
Завершается проверка узла.
```

Пример для клиента Windows

Убедиться, что определение узла SUSAN правильно создано в файле `client-configuration.xml`.

Введите указанную ниже команду из каталога `C:\Program Files\Tivoli\TSM\cms\bin`:

Команды:
```
cmsconfig verify SUSAN
```

Во время проверки вас попросят ввести имя клиентского узла или ID администратора и пароль.

Выходные результаты:

```
Проверка узла.


Проверка конфигурации службы CMS для узла SUSAN.
Конфигурация CMS правильная.

Проверка правильности работы службы CMS на порту 9028.

Введите ваш ID пользователя: admin
Введите ваш пароль:

Устанавливается соединение со службой CMS и проверяются ресурсы.
Служба CMS работает правильно.
Завершается проверка узла.
```

Команда CmsConfig list

Команда **CmsConfig list** показывает конфигурацию службы управления клиентом.

Синтаксис

Пример для клиента Linux

Показать конфигурацию службы управления клиентом. После этого просмотрите выходные результаты, чтобы убедиться, что команда введена правильно.

Введите из каталога `/opt/tivoli/tsm/cms/bin` следующую команду:

Команда:

```
./CmsConfig.sh list
```

Выходные результаты:

```
Список конфигурации CMS

server.example.com:1500 NO_SSL SUSAN
Возможности: [LOG_QUERY]
    Путь опций: /opt/tivoli/tsm/client/ba/bin/dsm.sys

    Файл журнала: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252

    Файл журнала: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

Пример для клиента Windows

Показать конфигурацию службы управления клиентом. После этого просмотрите выходные результаты, чтобы убедиться, что команда введена правильно.

Введите указанную ниже команду из каталога `C:\Program Files\Tivoli\TSM\cms\bin`:

Команда:

```
cmsconfig list
```

Выходные результаты:

```
Список конфигурации CMS

server.example.com:1500 NO_SSL SUSAN
Возможности: [LOG_QUERY]
    Путь опций: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

    Файл журнала: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252

    Файл журнала: C:\Program Files\Tivoli\TSM\baclient\dsmsched.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

Команда CmsConfig help

Используйте команду **CmsConfig help**, чтобы увидеть синтаксис команд утилиты **CmsConfig**.

Синтаксис

Пример для клиента Linux

Введите из каталога `/opt/tivoli/tsm/cms/bin` следующую команду:

```
./CmsConfig help
```

Пример для клиента Windows

Введите указанную ниже команду из каталога `C:\Program Files\Tivoli\TSM\cms\bin`:

```
CmsConfig help
```

Дополнительные возможности компонента служба управления клиентами

По умолчанию, компонент IBM Spectrum Protect служба управления клиентами собирает информацию только из файлов журналов клиента. Чтобы инициировать другие действия клиента, можно получить доступ к API Representational State Transfer (REST), включенному в компонент служба управления клиентами.

Разработчик API может создать приложения REST, чтобы инициировать следующие действия клиента:

- Запросить и обновить файлы опций клиента (например, файл `dsm.sys` на клиентах Linux и файл `dsm.opt` на клиентах Linux и Windows).
- Запросить состояние демона client acceptor и планировщика IBM Spectrum Protect.
- Создать резервные копии файлов и восстановить файлы для клиенртского узла.
- Расширить возможности компонента служба управления клиентами с использованием сценариев.

Подробную информацию о служба управления клиентами REST API смотрите в публикации Client Management Services REST API Guide (Руководство по REST API служб управления клиента).

Глава 12. Устранение неполадок установки Центра операций

Если в процессе установки Центра операций возникает проблема, которую вы не можете решить, вы можете поискать возможное решение в описаниях уже известных проблем.

Китайский, японский или корейский шрифты неправильно выводятся

Китайский, японский или корейский шрифты неправильно выводятся в компоненте Центр операций в Red Hat Enterprise Linux 5.

Решение

Установите следующие пакеты шрифтов (их можно получить от Red Hat):

- fonts-chinese
- fonts-japanese
- fonts-korean

Глава 13. Удаление компонента Центр операций

Центр операций можно деинсталлировать любым из следующих методов: графический мастер, командная строка в режиме консоли или режим без вывода сообщений.

Деинсталляция Центра операций при помощи графического мастера

Центр операций можно деинсталлировать при помощи графического мастера IBM Installation Manager.

Процедура

1. Откройте IBM Installation Manager.

   В каталоге, в котором установлен IBM Installation Manager, перейдите в подкаталог `eclipse` (например, `/opt/IBM/InstallationManager/eclipse`) и введите следующую команду:

   ```
   ./IBMIM
   ```

2. Щелкните по **Деинсталлировать**.
3. Выберите опцию для Центра операций и нажмите кнопку **Далее**.
4. Щелкните по **Деинсталлировать**.
5. Щелкните по **Готово**.

Деинсталляция Центра операций в режиме консоли

Чтобы деинсталлировать Центр операций из командной строки, запустите программу деинсталляции IBM Installation Manager из командной строки, указав параметр для режима консоли.

Процедура

1. В каталоге, в котором установлен IBM Installation Manager, перейдите в следующий подкаталог:

   ```
   eclipse/tools
   ```

   Например:

   ```
   /opt/IBM/InstallationManager/eclipse/tools
   ```

2. В каталоге `tools` введите следующую команду:

   ```
   ./imcl -c
   ```

3. Для деинсталляции введите 5.
4. Выберите деинсталляцию в группе пакетов IBM Spectrum Protect.
5. Введите N (Next - Далее).
6. Выберите деинсталляцию пакета компонента Центр операций.
7. Введите N (Next - Далее).
8. Введите U (Uninstall - Деинсталляция).
9. Введите F (Finish - Готово).

Деинсталляция Центра операций в режиме без вывода сообщений

Чтобы деинсталлировать Центр операций в режиме без вывода сообщений, запустите программу деинсталляции IBM Installation Manager из командной строки, указав параметры для режима без вывода сообщений.

Прежде чем начать

Вы можете использовать файл ответов, чтобы задать входные данные для деинсталляции сервера Центра операций в режиме без вывода сообщений. IBM Spectrum Protect содержит пример файла ответов, `uninstall_response_sample.xml`, в каталоге `input` в том месте, куда был распакован пакет установки. Этот файл содержит значения по умолчанию, которые помогут вам избежать ненужных предупреждений.

Чтобы деинсталлировать Центр операций, оставьте заданное значение `modify="false"` для записи Центра операций в файле ответов.

Если вы хотите настроить файл ответов, вы можете изменить опции, содержащиеся в файле. Информацию о файлах ответов смотрите в разделе Файлы ответов.

Процедура

1. В каталоге, в котором установлен IBM Installation Manager, перейдите в следующий подкаталог:

   ```
   eclipse/tools
   ```

   Например:

   ```
   /opt/IBM/InstallationManager/eclipse/tools
   ```

2. В каталоге `tools` введите следующую команду, где *файл_ответов* - это полное имя файла ответов:

   ```
   ./imcl -input файл_ответов -silent
   ```

   Пример команды:

   ```
   ./imcl -input /tmp/input/uninstall_response.xml -silent
   ```

Глава 14. Откат к предыдущей версии Центра операций

По умолчанию IBM Installation Manager сохраняет предыдущие версии пакетов для выполнения отката, если с более поздними версиями обновлений, исправлений или пакетов возникает проблема.

Прежде чем начать

Функция отката доступна только после обновления Центра операций.

Об этой задаче

Если IBM Installation Manager выполняет откат пакета до предыдущей версии, то текущая версия файлов пакета деинсталлируется, а более ранняя версия переустанавливается.

Чтобы выполнить откат к предыдущей версии Центра операций, IBM Installation Manager необходим доступ к файлам для этой версии. По умолчанию эти файлы сохраняются при каждой очередной установке. Поскольку число сохраненных файлов увеличивается с каждой установленной версией, вам может потребоваться удалять эти файлы из системы в соответствии с расписанием. Однако если вы удаляете эти файлы, вы не сможете выполнить откат на предыдущую версию.

Чтобы удалить сохраненные файлы или изменить ваши предпочтения относительно сохранения этих файлов в будущих установках, выполните следующие действия:

1. В IBM Installation Manager выберите **Файл** > **Предпочтения**.
2. На странице **Предпочтения** щелкните по **Файлы для отката** и укажите свои предпочтения.

Процедура

- Чтобы выполнить откат к предыдущей версии Центра операций, используйте функцию **Откат** программы IBM Installation Manager.

Приложение A. Файлы журнала установки

Если в процессе установки возникают ошибки, то они записываются в файлы журнала, которые находятся в каталоге журналов IBM Installation Manager.

Вы можете просмотреть файлы журнала установки, выбрав **Файл** > **Просмотреть журнал** в инструменте Installation Manager. Чтобы выполнить сбор этих файлов журнала, выберите **Справка** > **Экспорт данных для анализа проблем** в инструменте Installation Manager.

Приложение B. 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 (www.w3.org/TR/wai-aria/), чтобы обеспечить соответствие разделу US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) и рекомендациям по доступности веб-содержимого (Web Content Accessibility Guidelines (WCAG) 2.0 (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 (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 TTY для использования глухими или слабо слышащими заказчиками с целью получения доступа к службам продаж и поддержки:

Служба TTY
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 (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.

Зарегистрированный товарный знак Linux используется согласно сублицензии от Linux Foundation, исключительного лицензиата Линуса Торвальдса, который является владельцем этого знака во всем мире.

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.

Red Hat, OpenShift®, Ansible® и Ceph® - товарные знаки или зарегистрированные товарные знаки Red Hat, Inc. или филиалов этой компании в США и других странах.

UNIX - зарегистрированный товарный знак The Open Group в США и других странах.

VMware, VMware vCenter Server и VMware vSphere - зарегистрированные товарные знаки VMware, Inc. или филиалов этой компании в США и/или на территориях под другой юрисдикцией.

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

А

Б

В

Г

Д

Ж

З

И

К

Л

М

Н

О

П

P

C

Т

У

Ф

Х

Ц

Э

Я

Номер программы: 5725-W99
5725-W98
5725-X15