



System i

Готовность:

Обеспечение высокой готовности
с помощью задач

Версия 6, выпуск 1





System i

Готовность:

Обеспечение высокой готовности
с помощью задач

Версия 6, выпуск 1

Замечание

Перед началом работы с этой информацией и с описанным в ней продуктом обязательно ознакомьтесь со сведениями, приведенными в разделе “Примечания”, на стр. 175.

Это издание относится к версии 6, выпуску 1, модификации 0 IBM i5/OS (код продукта 5761-SS1), а также ко всем последующим выпускам и модификациям, если в новых изданиях не будет указано обратное. Эта версия работает не на всех компьютерах с RISC-процессорами и не работает на компьютерах с CISC-процессорами.

© Copyright International Business Machines Corporation 1998, 2008. Все права защищены.

Содержание

Обеспечение высокой готовности с помощью задач 1

Планирование решения высокой готовности	2
Планирование устойчивости приложения	2
Определение устойчивых приложений	2
Архитектура i5/OS для приложений с поддержкой кластеров	2
Разработка кластерных приложений	3
Обеспечение устойчивости приложений	3
Перезапуск кластерных приложений высокой готовности	4
Вызов программы выхода для группы ресурсов кластера	5
CRG приложения	6
Управление устойчивыми IP-адресами CRG приложений	6
Пример: Действия при автоматическом переносе CRG приложений	8
Пример: Программа выхода приложения	9
Планирование устойчивости данных	47
Выбор данных, которые должны быть устойчивыми	47
Планирование переключаемых дисков	48
Требования к аппаратному обеспечению для переносимых дисков	48
Требования переносимых дисков к программному обеспечению	49
Требования к средствам связи для коммутируемого диска	49
Планирование распределенной по сайтам зеркальной защиты	49
Планирование географической зеркальной защиты	50
Планирование синхронного зеркального копирования	54
Планирование глобального зеркального копирования	57
Планирование логической репликации	61
Выбор систем для логической репликации	61
Партнеры IBM по разработке кластерных приложений и кластерные продукты	61
Планирование ведения журнала для логической репликации	62
Планирование резервного копирования для логической репликации	62
Планирование производительности для логической репликации	62
Планирование устойчивости среды	63
Планирование домена управления кластером	63
Планирование записей отслеживаемых ресурсов (MRE)	63
Планирование использования кластеров	63
Требования к аппаратному обеспечению в кластере	64

Требования к программному обеспечению в кластере	64
Требования к средствам связи в кластере	65
Организация выделенной сети для кластера	66
Советы: Средства связи кластера	66
Планирование производительности для кластеров	67
Планирование использования кластеров различных версий	69
Планирование производительности для кластеров	69
Таблица планирования для кластеров	70
Планирование FlashCopy	73
Требования к аппаратному обеспечению для FlashCopy	73
Требования FlashCopy к программному обеспечению	73
Требования к средствам связи для FlashCopy	73
Планирование защиты для высокой готовности	74
Рассылка информации по кластеру	74
Замечания по применению кластеров с брендмауэрами	74
Управление пользовательскими профайлами на узлах кластера	74
Настройка решения высокой готовности	75
Сценарии: Настройка высокой готовности	75
Сценарий: Переносимость диска между логическими разделами	75
Сценарий: Совместное использование коммутируемого диска системами	77
Сценарий: Коммутируемый диск с географической зеркальной защитой	78
Сценарий: Распределенная по сайтам зеркальная защита с географической зеркальной защитой	79
Сценарий: Распределенная по сайтам зеркальная защита с синхронным зеркальным копированием	81
Сценарий: Распределенная по сайтам зеркальная защита с глобальным зеркальным копированием	82
Настройка TCP/IP для высокой готовности	84
Настройка атрибутов конфигурации TCP/IP	85
Запуск сервера INETD	85
Настройка кластеров	85
Создание кластера	86
Подготовка узлов к добавлению в кластер	86
Добавление узлов	87
Запуск узлов	87
Добавление узла в домен устройств	88
Создание групп ресурсов кластера (CRG)	88
Запуск CRG	92
Задание очередей сообщений	92
Перенос ресурсов	94
Настройка узлов	95
Запуск узлов	95

Подготовка узлов к добавлению в кластер	95		Остановка CRG	125
Добавление узлов	96		Удаление CRG	126
Добавление узла в домен устройств	96		Создание переносимых устройств	126
Настройка CRG	97		Изменение домена восстановления для CRG	127
Запуск CRG	97		Управление событиями, вызывающими перенос ресурсов	128
Создание групп ресурсов кластера (CRG)	97		Управление доменом управления кластером	130
Настройка доменов управления кластером	101		Остановка административного домена кластера	132
Создание домена управления кластером	101		Удаление домена управления кластером	132
Добавление узла в домен управления кластером	102		Изменение свойств домена управления кластером	132
Запуск административного домена кластера	103		Управление записями отслеживаемых ресурсов	133
Синхронизация отслеживаемых ресурсов	103		Управление переносимыми дисками	149
Добавление записей отслеживаемых ресурсов	104		Запрет доступа к пулу дисков	149
Настройка коммутируемых дисков	105		Включение переносимости аппаратного обеспечения	150
Создание независимого ASP	105		Выполнение приостановки независимого пула дисков	152
Включение зеркальной защиты.	106		Возобновление работы независимого пула дисков	152
Выключение зеркальной защиты	107		Распределенное зеркальное копирование	152
Добавление накопителя или дискового пула	107		Управление географической зеркальной защитой	152
Оценка текущей конфигурации	108		Выключение географической зеркальной защиты	152
Настройка доступа к пулу дисков	109		Возобновление географической зеркальной защиты	153
Настройка распределенной по сайтам зеркальной защиты	110		Отсоединение зеркальной копии	154
Настройка географической зеркальной защиты	110		Присоединение зеркальной копии	155
Настройка сеанса синхронного зеркального копирования.	111		Удаление географической зеркальной защиты	156
Настройка сеанса глобального зеркального копирования.	111		Изменение свойств географической зеркальной защиты	156
Управление решением высокой готовности	112		Управление сеансами синхронного зеркального копирования	157
Сценарии: Управление решениями высокой готовности	112		Приостановка сеансов синхронного зеркального копирования	157
Сценарии: Выполнение резервного копирования в среде высокой готовности	112		Возобновление сеансов синхронного зеркального копирования	157
Сценарий: Резервное копирование в среде с географической зеркальной защитой	113		Удаление сеанса синхронного зеркального копирования.	158
Сценарий: Выполнение FlashCopy	113		Просмотр свойств синхронного зеркального копирования	158
Сценарий: Обновление операционной системы в среде высокой готовности	114		Управление глобальным зеркальным копированием	158
Пример: Обновление операционной системы	115		Приостановка сеансов глобального зеркального копирования	158
Сценарий: обеспечение высокой готовности устройств.	117		Возобновление сеансов глобального зеркального копирования	159
Управление кластерами	117		Удаление сеансов глобального зеркального копирования.	159
Коррекция версии кластера	118		Изменение свойств сеанса глобального зеркального копирования	159
Удаление кластера	118		Управление FlashCopy	160
Отображение конфигурации кластера	119		Настройка сеанса FlashCopy.	160
Сохранение и восстановление конфигурации кластера	119		Обновление FlashCopy	160
Мониторинг состояния кластера	120		Присоединение FlashCopy	161
Задание очередей сообщений	120		Отсоединение FlashCopy	161
Справочная таблица по удалению кластера	122			
Управление узлами	122			
Отображение свойств узла	122			
Завершение работы узлов	123			
Удаление узлов	123			
Удаление узла из домена устройств	124			
Управление группами ресурсов кластера (CRG)	124			
Отображение состояния CRG	124			

Удаление FlashCopy	161	Восстановление поврежденного объекта	
Восстановление данных из FlashCopy	161	кластера	171
Изменение свойств FlashCopy	162	Восстановление кластера после полного	
Устранение неполадок решения высокой готовности	162	выхода из строя	171
Устранение неполадок кластера	162	Восстановление кластера после аварии	172
Проверка работоспособности кластера	162	Восстановление кластера из резервной	
Сбор данных для восстановления кластера	164	копии	172
Наиболее частые неполадки кластеров	164	Устранение неполадок распределенной по сайтам	
Распад кластера	166	зеркальной защиты	172
Определение роли частей кластера после		Сообщения географической зеркальной	
распада	167	защиты	173
Перевод узлов после распада кластера в			
число неисправных.	168	Приложение. Примечания	175
Разделенные домены управления кластером	169	Информация об интерфейсе программирования	177
Советы: распад кластера	169	Товарные знаки.	177
Прочие неполадки	170	Условия и соглашения	177
Устранение последствий сбоя в заданиях			
кластера	170		

Обеспечение высокой готовности с помощью задач

Подход, предусматривающий настройку среды высокой готовности i5/OS с помощью задач, позволяет настроить решение высокой готовности в соответствии с требованиями бизнеса. Решение высокой готовности можно настроить с помощью графического интерфейса и командной строки.

В отличие от подхода на основе решений, в котором используется графический интерфейс Администратора решений высокой готовности и стандартное решение настраивается в автоматическом режиме с минимальным участием пользователя, подход на основе задач предоставляет опытным пользователям средства настройки и реализации собственного решения. Однако в этом случае для создания решения высокой готовности пользователь должен быть хорошо знаком с принципами работы и требованиями среды высокой готовности, а также несколькими интерфейсами.

Графический интерфейс Службы ресурсов кластера

Интерфейс Службы ресурсов кластера позволяет настроить технологии кластера, применяемые в решении высокой готовности, и управлять ими. Для работы с этим интерфейсом в системе должна быть установлена лицензионная программа IBM System i High Availability Solutions Manager (iHASM) 5761-HAS. С помощью этого интерфейса можно выполнить следующие операции:

- Создание кластера и управление им.
- Создание узлов и управление ими.
- Создание групп ресурсов кластера и управление ими.
- Создание административных доменов кластера и управление ими.
- Создание отслеживаемых ресурсов и управление ими.
- Отслеживание событий, связанных с кластером, таких как переключение и распад кластера.
- Выполнение принудительного переноса ресурсов во время плановых простоев, таких как запланированное обслуживание системы.

Интерфейс Управление дисками

Интерфейс Управление дисками позволяет настроить независимые пулы дисков, необходимые для реализации технологий обеспечения устойчивости данных, и управлять ими. В зависимости от типа выбранной технологии обеспечения устойчивости данных, может потребоваться выполнить следующие действия:

- Создать пул дисков
- Добавить пул в число используемых
- Удалить пул из числа используемых
- Настроить географическое зеркальное копирование
- Настроить синхронное зеркальное копирование
- Настроить глобальное зеркальное копирование

Командная строка

С помощью командной строки можно выполнить различные задачи настройки среды высокой готовности. Для каждой задачи, связанной с кластером, предусмотрена отдельная команда CL.

Информация, связанная с данной

Команды IBM System i High Availability Solutions Manager (iHASM)

Планирование решения высокой готовности

Перед настройкой решения высокой готовности i5/OS необходимо выполнить процедуру планирования, обеспечив тем самым выполнение всех требований.

Каждая технология обеспечения высокой готовности предъявляет минимальный набор требований, которые должны быть выполнены для настройки конкретного решения. Помимо этих требований важно определить, какие именно ресурсы должны быть устойчивыми. Оцените ресурсы (приложения, данные и устройства) и определите, следует ли добавить их в решение высокой готовности. Если требуется обеспечить высокую готовность ресурсов, то перед настройкой решения высокой готовности важно внести все необходимые изменения в среду. Например, если требуется обеспечить высокую готовность данных из библиотеки SYSBAS, то перед настройкой решения данные следует перенести в независимый пул дисков. Приложения также может потребоваться изменить для обеспечения высокой готовности.

Планирование устойчивости приложения

Устойчивость приложения - один из краеугольных камней среды высокой готовности. Если вы планируете разрабатывать и применять в кластере приложения с высокой готовностью, то следует помнить, что для таких приложений существуют свои требования к готовности.

Устойчивые приложения можно перезапускать на разных узлах кластера без изменения конфигурации клиентов. При сбое или переносе приложения на другой узел сохраняются его данные. Для пользователя переключение приложения с основного на резервный узел происходит практически незаметно. С точки зрения пользователя совершенно безразлично, где именно выполняется приложение.

Для обеспечения устойчивости приложений в кластере необходимо, чтобы все приложения соответствовали ряду требований. Часть этих требований нужна для возможности переключения приложений - основной операции, гарантирующей постоянную готовность приложений для пользователей. Эти требования можно выполнить различными способами:

1. Приобрести приложение с поддержкой кластеров

Продукты с поддержкой кластеров отвечают требованиям высокой готовности.

2. Разработать или адаптировать приложение с учетом требований высокой готовности

Независимые разработчики программного обеспечения могут самостоятельно адаптировать приложения для применения их в среде высокой готовности i5/OS в качестве перемещаемых приложений.

После создания устойчивого приложения его работой должен управлять кластер.

Информация, связанная с данной

Высокая готовность и кластеры

Определение устойчивых приложений

Далеко не все приложения могут воспользоваться преимуществами кластеров.

Прежде всего, приложение должно обладать свойством устойчивости - только тогда для него будет возможен автоматический или принудительный перенос. Устойчивые приложения можно перемещать на резервные узлы без перенастройки клиентов. Для того чтобы приложение было устойчивым, оно должно удовлетворять ряду требований.

Архитектура i5/OS для приложений с поддержкой кластеров

В приложениях высокой готовности, сохраняющих устойчивость практически при любом сбое, предусматривается дополнительное значение конечного пользователя.

В системе i5/OS применяется архитектура устойчивых приложений, поддерживающая различные уровни приложений высокой готовности. Приложения самого высокого уровня этого диапазона демонстрируют характеристики высокой готовности, обеспечивают автоматизацию среды высокой готовности и управляются с помощью интерфейсов управления высокой готовности.

Данные приложения обладают следующими характеристиками:

- Приложение может быть автоматически перенесено на резервный узел кластера в случае выхода главного узла из строя.
- Приложение создает устойчивую среду в соответствии с формальными требованиями к устойчивости и поддерживает автоматическую настройку и запуск посредством службы ресурсов кластера.
- Устойчивость приложения обеспечивается программой выхода CRG приложений, которая обрабатывает события кластера с помощью функций службы ресурсов кластера i5/OS.
- В приложении предусмотрена функция перезапуска, перенаправляющая пользователя в главное меню приложения или его аналог.

Приложения с более ограниченными возможностями по доступности и перезапуску, обладают следующими характеристиками:

- Устойчивость приложения повышается за счет максимально тщательной обработки событий кластера с помощью программы выхода.
- Приложение предоставляет расширенные возможности по перезапуску. Для приложений, ориентированных на сервер, это означает, что пользователь после перезапуска должен оказаться на границе последней выполненной транзакции управления фиксацией или на последней установленной контрольной точке. Для приложений, ориентированных на клиентские системы, это означает, что перезапуск приложения должен произойти полностью прозрачно для пользователя, при этом прерывание работы приложения будет минимальным.

Разработка кластерных приложений

Кластерные приложения, для которых гарантирована устойчивость при выходе системы из строя, иногда называют приложениями с высокой готовностью.

Различают разные уровни готовности:

1. Если в приложении возникает ошибка, приложение перезапускает себя на том же узле кластера и устраняет возможные причины ошибок (например, ошибки в управляющих данных). С точки зрения пользователя это будет выглядеть так, как будто приложение запущено в первый раз.
2. В приложении предусмотрена ограниченная поддержка возобновления работы с контрольных точек. С точки зрения пользователя это выглядит так, как будто приложение немного вернулось назад от точки сбоя.
3. При выходе системы из строя приложение перезапускается на резервном сервере. С точки зрения пользователя это будет выглядеть так, как будто приложение запущено в первый раз.
4. При выходе системы из строя приложение перезапускается на резервном сервере и выполняет ограниченные действия по обработке контрольных точек и возобновлению работы. С точки зрения пользователя это выглядит так, как будто приложение немного вернулось назад от точки сбоя.
5. При выходе системы из строя на резервный узел переносится не только приложение, но и его данные. С точки зрения пользователя это будет выглядеть так, как будто приложение запущено в первый раз.
6. При выходе системы из строя на резервный узел переносится не только приложение, но и его данные. Помимо этого, приложение ограничено поддерживает возобновления работы с контрольных точек. С точки зрения пользователя это выглядит так, как будто приложение немного вернулось назад от точки сбоя.

Примечание: В вариантах 1-4 ответственность за сохранность данных ложится на пользователя.

Обеспечение устойчивости приложений:

Обеспечение устойчивости приложений.

Устойчивым называется приложение, отвечающее следующим требованиям:

- Приложение можно перезапустить на данном или любом другом узле
- Приложение доступно клиенту по IP-адресу

- Если в приложении предусмотрены состояния, доступны сведения о состоянии
- Данные приложения доступны после восстановления приложения в случае сбоя

Устойчивость приложения в кластерной среде в основном зависит от следующих главных составляющих:

Само приложение

Как сильно может повлиять сбой системы на работу приложения, и может ли приложение самостоятельно перезапуститься?

Эту задачу можно решить с помощью кластерных технологий.

Связанные данные

Может ли сбой системы привести к потере данных?

Важные данные можно хранить на коммутируемых дисках, которые обеспечивают доступность данных даже при простое. Сохранность данных в случае сбоя можно обеспечить с помощью продукта копирования для кластеров делового партнера фирмы IBM .

Управление возможностями и администрирование

Насколько просто создать среду, в которой будет обеспечена высокая готовность данных и приложения?

IBM System i High Availability Solutions Manager (iHASM), лицензионный номер программы (5761-HAS), предоставляет несколько интерфейсов для настройки и управления решениями и технологиями высокой готовности. Лицензионная программа iHASM предоставляет следующие интерфейсы:

Графический интерфейс Администратора решений высокой готовности

Этот графический интерфейс позволяет выбирать из нескольких решений высокой готовности, поддерживаемых i5/OS. Он оценивает все технологические требования для выбранного решения, настраивает его и связанные с ним технологии и обеспечивает упрощенное управления всеми технологиями высокой готовности, из которых состоит решение.

Графический интерфейс Службы ресурсов кластера

Этот графический интерфейс обеспечивает опытному пользователю большую гибкость при пользовательской настройке решения высокой готовности. Он позволяет настраивать и управлять технологиями кластера, например, CRG. Также из него можно настроить несколько независимых ASP, которые будут использоваться как часть решения высокой готовности.

Команды Администратора решений высокой готовности IBM для System i

Эти команды обеспечивают похожие функции, но доступ к ним осуществляется через интерфейс командной строки.

API Администратора решений высокой готовности IBM для System i

Данные API позволяют работать с новой функцией настройки независимых ASP.

Также можно использовать интерфейс управления кластерами, работающий с кластерными API и совмещающий устойчивые приложения с устойчивыми данными, от сторонних производителей.

Информация, связанная с данной

Управление средой высокой готовности

Перезапуск кластерных приложений высокой готовности:

Для перезапуска приложения требуется, чтобы на момент начала автоматического или принудительного переноса приложению было известно его состояние.

Состав сведений о состоянии зависит от конкретного приложения, поэтому приложение самостоятельно устанавливает перечень того, что ему нужно. В отсутствие информации о состоянии приложение можно перезапустить с РС. Однако, необходимо вновь установить свое положение в приложении.

Сведения о состоянии приложения можно сохранять и передавать в резервную систему разными способами. При выборе подходящего способа следует учитывать особенности конкретного приложения.

- Приложение может передавать полные сведения о состоянии в запрашивающую систему клиента. При автоматическом или принудительном переносе ресурсов на новом сервере восстанавливается последнее известное состояние приложения. Для реализации этого метода можно воспользоваться API Разослать информацию или API группы Кластерная хэш-таблица.
- Приложение может осуществлять репликацию информации о состоянии (например, сведения о заданиях и прочих управляющих структурах) в режиме реального времени. При каждом изменении сведений приложение рассылает информацию об изменении в резервные системы.
- Приложение может хранить данные о состоянии в области данных программы выхода соответствующего CRG. Этот метод предполагает небольшой объем сохраняемой информации. Для реализации метода можно воспользоваться API Изменить группу ресурсов кластера (QcstChangeClusterResourceGroup).
- Приложение может хранить информацию о состоянии в объекте данных, для которого выполняется репликация.
- Приложение может хранить информацию о состоянии в объекте данных, содержащемся в переносимом независимом IASP и хранящем данные приложения.
- Приложение может хранить информацию о состоянии системы клиента.
- Приложение может не нуждаться в информации о состоянии.

Примечание: Правильное применение контрольных точек или их аналогов в приложении значительно сокращает потенциальный объем данных о состоянии, которые нужно хранить. Это связано с тем, что информацию о состоянии требуется сохранять только в ограниченном числе контрольных точек. Тогда при перезапуске приложения можно без труда выполнить откат на последнюю контрольную точку - подобно откату в службах фиксации баз данных.

Вызов программы выхода для группы ресурсов кластера:

Программа выхода группы ресурсов кластера вызывается при выполнении ряда операций в среде кластера.

Эта программа обеспечивает необходимую устойчивость для ресурсов кластера. Программу выхода не обязательно применять для CRG устойчивых устройств, но она нужна для других типов CRG. Программа выхода группы ресурсов кластера, если она применяется, вызывается при возникновении событий на уровне кластера, в том числе при выполнении следующих операций:

- Узел неожиданно выходит из кластера
- Узел выходит из кластера в результате вызова API Завершить работу узла кластера (QcstEndClusterNode) или API Удалить запись узла кластера (QcstRemoveClusterNodeEntry)
- Кластер удален в результате вызова API Удалить кластер (QcstDeleteCluster)
- Узел активируется в результате вызова API Запустить узел кластера (QcstStartClusterNode)
- Восстановлена связь с узлом, состоящим из нескольких разделов

Программа выхода выполняет следующие процессы:

- Выполняется в указанной группе активации или в группе активации вызывающего процесса (*CALLER).
- Игнорирует опцию перезапуска, если в программе выхода возникает непредвиденная исключительная ситуация, либо работа программы выхода отменяется.
- Предоставляет описатель для обеспечения возможности завершения работы программы выхода извне.

При выполнении API группы ресурсов кластера программа выхода запускается в отдельном задании под управлением пользовательского профайла, указанного в API Создать CRG (QcstCreateClusterResourceGroup).

API самостоятельно создает отдельное задание при запуске программы выхода. Если программа выхода для CRG данных завершится с ошибкой, то она еще раз вызывается на всех активных узлах домена восстановления с помощью кода действия Undo. В результате отменяются результаты всех незавершенных операций и восстанавливается исходное состояние группы ресурсов кластера.

Предположим, что произошел сбой принудительного переноса ресурсов для CRG устройства. После того как был осуществлен возврат на всех устройствах и если все они были успешно включены на исходном главном узле, кластер с помощью кода действия Start вызывает программу выхода на исходном главном узле.

Если возникнет ошибка в программе выхода CRG приложения, и при этом CRG будет активна, то служба ресурсов кластера попытается перезапустить приложение. Программа выхода CRG будет вызвана с помощью кода действия Restart. Если не удастся перезапустить приложение за отведенное число попыток, то программа выхода CRG будет вызвана с помощью кода действия Failover. Счетчик попыток обнуляется при вызове программы выхода с помощью кода действия Start, то есть при запуске CRG, сбое или переходе на другой узел.

При запуске группы ресурсов кластера программа выхода CRG, вызванная на главном узле, возвращает управление службе ресурсов кластера только после завершения приложения или возникновения ошибки. Если во время работы CRG приложения службе ресурсов кластера потребуется сообщить программе выхода CRG приложения о каком-либо событии, то будет запущен еще один экземпляр программы выхода в отдельном задании. Если код действия отличен от Start и Restart, то программа выхода возвращает управление сразу.

При вызове в программу выхода CRG передаются параметры, идентифицирующие кластер, текущее и ожидаемое состояние ресурсов кластера.

Полное описание программы выхода группы ресурсов кластера, включая параметры, передаваемые для каждого кода действия, приведено в разделе Программа выхода группы ресурсов кластера документации по API кластера. В библиотеке QUSRTOOL предусмотрен пример программы выхода, который можно использовать в качестве шаблона для создания собственных программ. См. элемент TCSTAPPEXT файла QATTSYSC.

CRG приложения

CRG приложения предназначена для обеспечения устойчивости приложений.

Управление устойчивыми IP-адресами CRG приложений:

Управление устойчивыми IP-адресами CRG приложений с помощью службы ресурсов кластера. Кроме того, предусмотрена возможность управления вручную.

Предусмотрено два способа управления IP-адресами CRG приложений. Простой способ (применяемый по умолчанию) заключается в том, что все управление берет на себя служба ресурсов кластера. В этом случае служба ресурсов кластера самостоятельно создает устойчивый IP-адрес для CRG приложений на всех узлах домена восстановления, включая узлы, которые добавляются в домен восстановления позднее. Этот способ предполагает, что устойчивый IP-адрес для CRG приложений не задан ни на одном узле домена восстановления.

Второй способ заключается в том, чтобы управлять устойчивыми IP-адресами вручную. В этом случае служба ресурсов кластера не принимает никакого участия в настройке устойчивых IP-адресов, и эта обязанность возлагается на пользователя. Устойчивый IP-адрес должен быть определен на всех узлах домена восстановления (за исключением узлов-копий) на момент включения CRG. Этот адрес также должен быть определен на всех узлах, добавляемых в домен восстановления CRG, на момент их добавления в домен.

Понятия, связанные с данным

“Пример: Действия при автоматическом переносе CRG приложений” на стр. 8

Данный пример демонстрирует, как работает один сценарий автоматического переноса. Могут применяться и другие процедуры.

Несколько подсетей: Теоретически применение устойчивого IP-адреса возможно даже в случае, если узлы домена восстановления распределены по нескольким подсетям. Для настройки устойчивого IP-адреса приложения, когда узлы в домене восстановления распространяются на несколько подсетей, необходимо активировать среду переноса ресурсов.

Перенос приложений за пределы локальной подсети:

В общем случае предполагается, что все узлы кластера, входящие в домен восстановления конкретной CRG, находятся в одной подсети. Служба ресурсов кластера позволяет при настройке CRG приложений вручную задавать устойчивые IP-адреса.

- | Для реализации виртуальных IP-адресов в пределах одной подсети применяются стандартные средства
- | протокола ARP. Однако если это необходимо, домен восстановления можно разнести по разным подсетям.
- | Для этого необходимо, чтобы на всех узлах домена восстановления, во всех подсетях домена восстановления
- | и на всех маршрутизаторах, установленных между ними, поддерживался усовершенствованный протокол
- | маршрутизации RIP.

Процедура настройки параметров переноса вручную приведена ниже. **Данные действия нужно выполнить на всех узлах домена восстановления и на прочих узлах кластера, которые будут входить в домен восстановления для данного CRG приложения.**

1. Выберите устойчивый IP-адрес для CRG приложения.
 - Во избежание конфликтов этот адрес не должен отличаться от всех других IP-адресов, используемых узлами кластера и маршрутизаторами. Например, если будет выбран адрес 19.19.19.19, то убедитесь, что 19.0.0.0 (19.19.0.0) не известны таблицам маршрутов системы.
 - Добавьте устойчивый интерфейс (например, 19.19.19.19) с описанием линии *VIRTUALIP, маской подсети 255.255.255.255 (маршрут к хосту), MTU 1500 (допустимы значения в диапазоне 576-16388) и параметром AUTOSTART(*NO). Этот адрес (например, 19.19.19.19) должен быть связан с линией *VIRTUALIP на момент выполнения следующего шага. Однако этот адрес не обязательно должен быть активным.
2. Свяжите устойчивый IP-адрес с одним или обоими IP-адресами, указанными для служб кластера при создании кластера или добавлении узла в кластер.
 - В нашем примере это означает, что адрес 19.19.19.19 нужно сделать связанным локальным интерфейсом для IP-адреса узла кластера на шине Ethernet для того, чтобы этот адрес мог применяться кластером. Эту операцию нужно выполнить на всех узлах кластера.

Примечание: В команде CFGTSP IP-адреса должны указываться полностью.

3. Создайте кластер и все необходимые CRG. Укажите для CRG приложений значение QcstUserCfgsTakeoverIpAddr в поле Устойчивый IP-адрес. Не запускайте пока CRG приложений.
4. Выберите в меню CFGTSP опцию 20 (Настроить приложения TCP/IP), затем опцию 2 (Настроить RouteD), затем 1 (Изменить атрибуты RouteD) и проверьте значение параметра Рассылать. Если оно отлично от *YES, укажите значение *YES и перезапустите демон ROUTED (RIP или RIP-2) на всех узлах кластера.
 - Если демон ROUTED работает, то опция 3 команды NETSTAT должна показать, что он подключен к локальному порту. На всех узлах домена восстановления CRG должен работать и рассылать информацию о маршрутах (параметр Рассылать = *YES) демон ROUTED.
5. Убедитесь в том, что все маршрутизаторы, установленные между узлами домена восстановления, получают и пересылают маршруты по протоколу RIP.
 - Этот режим далеко не всегда включен на маршрутизаторах. Производители используют разную терминологию, но так или иначе вам нужно включить режим пересылки данных о маршрутах к хостам и о динамических хостах по протоколу RIP.
 - Это относится как к интерфейсам маршрутизаторов, подключенным к системам, так и к интерфейсам, связывающим маршрутизаторы.

Примечание: Не используйте компьютер System i в качестве маршрутизатора в данной конфигурации. Вместо этого лучше приобретите отдельный маршрутизатор (IBM или сторонних производителей), предназначенный именно для эти целей. Средства маршрутизации System i не поддерживают данную функцию.

6. Активируйте устойчивый адрес вручную на одном из узлов кластера:
 - a. Подождите в течение 5 минут, чтобы все узлы получили по протоколу RIP сведения о расположении этого хоста.
 - b. Проверьте связь с устойчивым адресом со всех узлов домена восстановления CRG и прочих заинтересованных хостов в локальной сети, которые будут его использовать.
 - c. Убедитесь, что работа устойчивого адреса завершена.

(Кластер запустит IP-адрес на указанном главном узле при запуске CRG.)

7. Запустите CRG приложений.
 - Служба ресурсов кластера задействует устойчивый адрес на главном узле домена восстановления, а протокол RIP начнет рассылать информацию о расположении главного узла по домену восстановления. Примерно через 5 минут всем узлам домена восстановления будет известно расположение главного хоста. Протокол RIP сам по себе никак не связан с функцией запуска CRG.

Важная информация:

- Если процедура, приведенная выше, будет выполнена не для всех узлов домена восстановления CRG приложений, то попытка переноса ресурсов приведет к зависанию кластера.
- Хотя в данном примере не рассматривается возможность переноса данных на узлы копии, настоятельно рекомендуется разработать способ изменения роли узлов-копий на резервные узлы при необходимости. Тогда в критической ситуации узлы-копии смогут взять на себя роль главной точки доступа к ресурсам.
- Если применяется несколько виртуальных IP-адресов, то каждый из них должен быть связан с отдельной CRG приложений и отдельным неvirtуальным IP-адресом. Это может быть другой логический IP-адрес на том же физическом адаптере или на другом. Обязательно примите меры к предотвращению возникновения неоднозначности в таблицах маршрутов. Проще всего поступить так:
 - Добавьте маршрут *DFTRROUTE в таблицу маршрутизации для каждого виртуального IP-адреса.
 - Для использования множественного IP-адреса воспользуйтесь CFGTCP (опция 2).
 - Укажите все параметры, включая ближайший транзитный участок, и укажите в качестве предпочитаемой привязки IP-адрес локальной системы, связанный с данным виртуальным IP-адресом.

Пример: Действия при автоматическом переносе CRG приложений:

Данный пример демонстрирует, как работает один сценарий автоматического переноса. Могут применяться и другие процедуры.

При автоматическом переносе ресурсов CRG устойчивого приложения, сбой которого произошел из-за аварийного завершения задания или превышения числа попыток, происходит следующее:

- На всех активных узлах домена восстановления CRG вызывается программа выхода CRG с кодом действия failover. Служба ресурсов кластера готовится к автоматическому переносу точки доступа к приложению на первый резервный узел.
- Служба ресурсов кластера прерывает соединение IP с главным узлом CRG. Дополнительные сведения, касающиеся устойчивого IP-адреса.
- Служба ресурсов кластера переносит IP-адрес на первый резервный узел, который становится главным узлом.

- Служба ресурсов кластера запускает задание, которое вызывает на новом главном узле программу выхода CRG с кодом действия Start. Программа выхода перезапускает приложение.

Понятия, связанные с данным

“Управление устойчивыми IP-адресами CRG приложений” на стр. 6

Управление устойчивыми IP-адресами CRG приложений с помощью службы ресурсов кластера. Кроме того, предусмотрена возможность управления вручную.

Пример: Программа выхода приложения:

В этом примере содержится исходный код программы выхода группы ресурсов кластера приложений.

Данный пример исходного кода расположен в библиотеке QUSRTOOL.

Примечание: Используя приведенные примеры программ, вы обязуетесь соблюдать требования, изложенные в разделе “Лицензия на исходный код и отказ от обязательств” на стр. 173.

```

/*****/
/*
/* Библиотека: QUSRTOOL
/* Файл: QATTSYSC
/* Элемент: TCSTAPPEXT
/* Тип: ILE C
/*
/* Описание:
/* Это пример программы выхода CRG приложений, которая вызывается для
/* обработки различных событий кластера, а также для API кластера. В
/* этот пример необходимо добавить дополнительные процедуры, так
/* как они в значительной степени зависят от уникальных действий,
/* выполняемых для каждого конкретного приложения.
/*
/* С помощью этого примера создается оболочка, содержащая основу
/* для создания программы выхода CRG. Комментарии, приведенные в этом
/* примере, описывают те вопросы, на которые необходимо
/* обратить внимание при создании реальной программы выхода.
/*
/* В этом примере обрабатываются все коды действий,
/* допустимые для CRG приложений.
/*
/* Включаемый файл tcstdtaara.h также входит в состав библиотеки QUSRTOOL.
/* См. элемент TCSTDTAARA в файле QATTSYSC.
/*
/* Протокол изменений:
/* Флаг Причина Версия Дата ИД польз. Описание
/*
/* ... D98332 v5r1m0 000509 ROCH Начальное создание
/* $A1 P9950070 v5r2m0 010710 ROCH Исправления области данных
/* $A2 D99055 v5r2m0 010913 ROCH Добавлен код действия CancelFailover*/
/* $A3 D98854 v5r2m0 010913 ROCH Добавлен код действия VerificationPhase*/
/* $A4 P9A10488 v5r3m0 020524 ROCH Добавлен код примера ожидания данных*/
/* Код действия CRG при переносе
/*
/*****/

/*-----*/
/*
/* Заголовочные файлы
/*
/*-----*/
#include /* Полезно при отладке */
#include /* макрос offsetof */
#include /* системная функция */
#include /* строковые функции */
#include /* константы/структуры обработки исключительных ситуаций */

```

```

#include          /* различные константы кластера          */
#include          /* структура информации CRG          */
#include "qusrtool/qattdata/qattdata" /* области данных QCSTHAAPPI/QCSTHAAPPO*/
#include          /* API для извлечения содержимого из области данных */
#include          /* API определения типа кода ошибки          */
#include          /* встроенная функция mitime          */
#include          /* встроенная функция waittime          */

/*-----*/
/*
/* Константы
/*
/*-----*/
#define UnknownRole -999
#define DependCrgDataArea "QCSTHAAPPO"
#define ApplCrgDataArea "QCSTHAAPPI"
#define Nulls 0x000000000000000000000000

/*-----*/
/*
/* Приведенные ниже константы используются в функции checkDependCrgDataArea().*/
/* Первая из них определяет время ожидания перед проверкой области
/* данных. Вторая задает максимальное время ожидания готовности области данных*/
/* при выполнении функции Запустить CRG, перед отменой запуска приложения.
/* Третья задает максимальное время ожидания для функций Выполнить
/* принудительный перенос ресурсов или Выполнить автоматический перенос ресурсов.
/*-----*/
#define WaitSecondsIncrement 30
#define MaxStartCrgWaitSeconds 0
#define MaxWaitSeconds 900

/*-----*/
/*
/* Так как данная программа выхода позволяет обрабатывать новые
/* коды действий, измените значение, приведенное ниже, на
/* наибольший код обрабатываемого действия.
/*-----*/
#define MaxAc 21

/*-----*/
/*
/* Если данные программы выхода в CRG обладают определенной структурой,
/* включите заголовочный файл, в котором содержится определение этой
/* структуры и укажите в следующей строке вместо char имя этой структуры.
/*-----*/
#define EpData char

/*-----*/
/*
/* Укажите в следующей строке имя библиотеки, в которой содержится
/* приложение и где будут находиться области данных QCSTHAAPPO и
/* QCSTHAAPPI.
/*-----*/
#define ApplLib "QGPL"

/*-----*/
/*
/* Прототипы внешних функций.
/*
/*-----*/

```

```

static int getMyRole(Qcst_EXTP0100_t *, int, int);
#pragma argopt(getMyRole)
static int doAction(int, int, int, Qcst_EXTP0100_t *, EpData *);
#pragma argopt(doAction)
static int createCrg(int, int, Qcst_EXTP0100_t *, EpData *);
static int startCrg(int, int, Qcst_EXTP0100_t *, EpData *);
static int restartCrg(int, int, Qcst_EXTP0100_t *, EpData *);
static int endCrg(int, int, Qcst_EXTP0100_t *, EpData *);
static int verifyPhase(int, int, Qcst_EXTP0100_t *, EpData *);
static int deleteCrg(int, int, Qcst_EXTP0100_t *, EpData *);
static int memberIsJoining(int, int, Qcst_EXTP0100_t *, EpData *);
static int memberIsLeaving(int, int, Qcst_EXTP0100_t *, EpData *);
static int switchPrimary(int, int, Qcst_EXTP0100_t *, EpData *);
static int addNode(int, int, Qcst_EXTP0100_t *, EpData *);
static int rmvNode(int, int, Qcst_EXTP0100_t *, EpData *);
static int chgCrg(int, int, Qcst_EXTP0100_t *, EpData *);
static int deleteCrgWithCmd(int, int, Qcst_EXTP0100_t *, EpData *);
static int undoPriorAction(int, int, Qcst_EXTP0100_t *, EpData *);
static int endNode(int, int, Qcst_EXTP0100_t *, EpData *);
static int chgNodeStatus(int, int, Qcst_EXTP0100_t *, EpData *);
static int cancelFailover(int, int, Qcst_EXTP0100_t *, EpData *);
static int newActionCode(int, int, Qcst_EXTP0100_t *, EpData *);
static int undoCreateCrg(int, int, Qcst_EXTP0100_t *, EpData *);
static int undoStartCrg(int, int, Qcst_EXTP0100_t *, EpData *);
static int undoEndCrg(int, int, Qcst_EXTP0100_t *, EpData *);
static int undoMemberIsJoining(int, int, Qcst_EXTP0100_t *, EpData *);
static int undoMemberIsLeaving(int, int, Qcst_EXTP0100_t *, EpData *);
static int undoSwitchPrimary(int, int, Qcst_EXTP0100_t *, EpData *);
static int undoAddNode(int, int, Qcst_EXTP0100_t *, EpData *);
static int undoRmvNode(int, int, Qcst_EXTP0100_t *, EpData *);
static int undoChgCrg(int, int, Qcst_EXTP0100_t *, EpData *);
static int undoCancelFailover(int, int, Qcst_EXTP0100_t *, EpData *);
static void bldDataAreaName(char *, char *, char *);
#pragma argopt(bldDataAreaName)
static int checkDependCrgDataArea(unsigned int);
#pragma argopt(checkDependCrgDataArea)
static void setApp1CrgDataArea(char *);
#pragma argopt(setApp1CrgDataArea)
static void cancelHandler(_CNL_Hndlr_Parms_T *);
static void unexpectedExceptionHandler(_INTRPT_Hndlr_Parms_T *);
static void endApplication(unsigned int, int, int, Qcst_EXTP0100_t *, EpData *);
#pragma argopt(endApplication)

/*-----*/
/*
/* Процедуры отладки
/*
/*-----*/
static void printParms(int, int, int, Qcst_EXTP0100_t *, EpData *);
static void printActionCode(unsigned int);
static void printCrgStatus(int);
static void printRcvyDomain(char *,
                           unsigned int,
                           Qcst_Rcvy_Domain_Array1_t *);
static void printStr(char *, char *, unsigned int);

/*-----*/
/*
/* Определения типов
/*
/*-----*/

/*-----*/
/*
/* Эта структура определяет данные, передаваемые программам
/* обработки исключительных ситуаций и отмены заданий. Укажите в них
/*

```

```

/* информацию, уникальную для вашего приложения. */
/* */
/*-----*/
typedef struct {
    int *retCode; /* Указатель кода возврата */
    EpData *epData; /* Данные программы выхода от CRG */
    Qcst_EXTP0100_t *crgData; /* Данные CRG */
    unsigned int actionCode; /* Код действия */
    int role; /* Роль этого узла в домене восстановления */
    int priorRole; /* Предыдущая роль этого узла в домене восстановления*/
} volatile HandlerDataT;

/*-----*/
/* */
/* Массив указателей на функции, обрабатывающие коды действий. */
/* Если программа выхода обновляется для обработки кодов новых действий, */
/* добавьте имена новых функций в этот массив указателей на функции. */
/* */
/*-----*/
static int (*fcn[MaxAc+1]) (int role,
                            int priorRole,
                            Qcst_EXTP0100_t *crgData,
                            EpData *epData) = {
    newActionCode, /* 0 - зарезервировано */
    createCrg, /* 1 */
    startCrg, /* 2 */
    restartCrg, /* 3 */
    endCrg, /* 4 */
    verifyPhase, /* 5 - зарезервировано */
    newActionCode, /* 6 - зарезервировано */
    deleteCrg, /* 7 */
    memberIsJoining, /* 8 */
    memberIsLeaving, /* 9 */
    switchPrimary, /* 10 */
    addNode, /* 11 */
    rmvNode, /* 12 */
    chgCrg, /* 13 */
    deleteCrgWithCmd, /* 14 */
    undoPriorAction, /* 15 */
    endNode, /* 16 */
    newActionCode, /* 17 - предназначено только для CRG устройств */
    newActionCode, /* 18 - предназначено только для CRG устройств */
    newActionCode, /* 19 - предназначено только для CRG устройств */
    chgNodeStatus, /* 20 */
    cancelFailover /* 21 */
};

/*-----*/
/* */
/* Массив указателей на функции для обработки предыдущих кодов */
/* действий, в случае вызова совместно с кодом действия Отменить. */
/* Если программа выхода обновляется для обработки действия */
/* Отмена с новыми кодами действий, добавьте имена новых */
/* функций в этот массив указателей на функции. */
/* */
/*-----*/
static int (*undoFcn[MaxAc+1]) (int role,
                                int priorRole,
                                Qcst_EXTP0100_t *crgData,
                                EpData *epData) = {
    newActionCode, /* 0 - зарезервировано */
    undoCreateCrg, /* 1 */
    undoStartCrg, /* 2 */
    newActionCode, /* 3 */
    undoEndCrg, /* 4 */
};

```

```

newActionCode,      /* 5 - для действия с эти кодом отмена не выполняется */
newActionCode,      /* 6 - зарезервировано */
newActionCode,      /* 7 */
undoMemberIsJoining, /* 8 */
undoMemberIsLeaving, /* 9 */
undoSwitchPrimary,  /* 10 */
undoAddNode,        /* 11 */
undoRmvNode,        /* 12 */
undoChgCrg,         /* 13 */
newActionCode,      /* 14 */
newActionCode,      /* 15 */
newActionCode,      /* 16 */
newActionCode,      /* 17 - предназначено только для CRG устройств */
newActionCode,      /* 18 - предназначено только для CRG устройств */
newActionCode,      /* 19 - предназначено только для CRG устройств */
newActionCode,      /* 20 */
undoCancelFailover /* 21 */
};

/*****
/*
/* Это точка входа для программы выхода.
/*
/*
*****/
void main(int argc, char *argv[]) {

    HandlerDataT hdldata;

/*----- */
/*
/* Преобразует все аргументы, переданные в массив argv, в данные
/* соответствующих типов.
/*
/*----- */
    int *retCode = (int *)argv[1];
    unsigned int *actionCode = (unsigned int *)argv[2];
    EpData *epData = (EpData *)argv[3];
    Qcst_EXTP0100_t *crgData = (Qcst_EXTP0100_t *)argv[4];
    char *formatName = (char *)argv[5];

/*----- */
/*
/* Проверяет, верен ли формат передаваемых данных.
/* Если нет, то вносится изменение, при этом данную программу выхода
/* необходимо соответствующим образом обновить. Добавляет в приложение
/* функцию ведения протокола ошибок.
/*
/*----- */
    if (0 != memcmp(formatName, "EXTP0100", 8))
        abort();

/*----- */
/*
/* Укажите данные, которые будут передаваться программам обработки
/* исключительных ситуаций и отмены.
/*
/*----- */
    hdldata.retCode = retCode;
    hdldata.epData = epData;

```

```

hdlData.crgData    = crgData;
hdlData.actionCode = *actionCode;
hdlData.role       = UnknownRole;
hdlData.priorRole  = UnknownRole;
_VBDY(); /* принудительно записывать измененные переменные в основное расположение */

/*-----*/
/*
/* Применять программу обработки исключительных ситуаций для всех
/* исключительных ситуаций.
/*
/*-----*/
#pragma exception_handler(unexpectedExceptionHandler, hdlData, \
                        _C1_ALL, _C2_ALL, _CTLA_INVOKE )

/*-----*/
/*
/* Применяется обработка отмены заданий для восстановления в случае отмены этого задания.
/*
/*-----*/
#pragma cancel_handler(cancelHandler, hdlData)

/*-----*/
/*
/* Извлечение текущей и предыдущей ролей узла, на котором выполняется
/* программа выхода. Если API кластера или событие изменяет домен
/* восстановления (роль узла или членство), то новое смещение домена
/* восстановления передается в Offset_Rcvy_Domain_Array, а смещение
/* домена восстановления до изменения передается в массив
/* Offset_Prior_Rcvy_Domain_Array. Если домен восстановления не изменен,
/* то к нему можно обратиться только через Offset_Rcvy_Domain_Array.
/*
/*-----*/
hdlData.role = getMyRole(crgData,
                        crgData->Offset_Rcvy_Domain_Array,
                        crgData->Number_Nodes_Rcvy_Domain);
if (crgData->Offset_Prior_Rcvy_Domain_Array)
    hdlData.priorRole =
        getMyRole(crgData,
                  crgData->Offset_Prior_Rcvy_Domain_Array,
                  crgData->Number_Nodes_Prior_Rcvy_Domain);
else
    hdlData.priorRole = hdlData.role;
_VBDY(); /* принудительно записывать измененные переменные в основное расположение */

/*-----*/
/*
/* Для печати информации отладки разрешите следующую строку.
/*
/*-----*/
printParms(*actionCode, hdlData.role, hdlData.priorRole, crgData,
epData);
*/

```

```

/*-----*/
/*
/* Позволяет не вносить изменения на основе кода действия. Код
/* возврата задается в соответствии с результатом функции doAction().
/*
/*-----*/

*retCode = doAction(*actionCode,
                    hdlData.role,
                    hdlData.priorRole,
                    crgData,
                    epData);

/*-----*/
/*
/* Задание программы выхода завершается, если в этой точке управление
/* возвращается операционной системе.
/*
/*-----*/

return;

#pragma disable_handler /* unexpectedExceptionHandler */
#pragma disable_handler /* cancelHandler */
} /* конец функции main()

/*****
/*
/* Получить роль этого узла из представления домена восстановления.
/*
/* Следующие API и события кластера передают программе выхода
/* обновленный и предыдущий домен восстановления:
/* QcstAddNodeToRcvyDomain
/* QcstChangeClusterNodeEntry
/* QcstChangeClusterResourceGroup
/* QcstEndClusterNode (завершаемый узел не получает домен восстановления)
/* QcstInitiateSwitchOver
/* QcstRemoveClusterNodeEntry (удаленный узел не получает домен восстановления)
/* QcstRemoveNodeFromRcvyDomain
/* QcstStartClusterResourceGroup (если изменяется порядок неактивных
/* резервных узлов)
/* сбой, который привел к автоматическому переносу ресурсов
/* узел, который возвращается в кластер
/* объединение разделов кластера
/*
/* Все остальные API передают только обновленный домен восстановления.
/*
/*****
static int getMyRole(Qcst_EXTP0100_t *crgData, int offset, int count) {
Qcst_Rcvy_Domain_Array1_t *nodeData;
    unsigned int iter = 0;

/*-----*/
/*
/* В некоторых случаях операционная система не может определить ИД узла
/* и передает значение *NONE. Например, если в узле неактивны службы
/* ресурсов кластера и применяется команда CL DLTCRG.
/*
/*-----*/

if (0 == memcmp(crgData->This_Nodes_ID, QcstNone,
sizeof(Qcst_Node_Id_t)))
    return UnknownRole;

```

```

/*-----*/
/*
/* Вычисление указателя на первый элемент массива домена восстановления. */
/*
/*-----*/

nodeData = (Qcst_Rcvy_Domain_Array1_t *)((char *)crgData + offset);
/*-----*/
/*
/* Поиск узла в массиве домена восстановления. При добавлении узла с
/* помощью API добавления узла в домен восстановления, он не будет найден*/
/* в предыдущем домене восстановления.
/*
/*-----*/

while ( 0 != memcmp(crgData->This_Nodes_ID,
                  nodeData->Node_ID,
                  sizeof(Qcst_Node_Id_t))
        &&
        iter < count
    ) {
    nodeData++;
    iter++;
}

if (iter < count)
    return nodeData->Node_Role;
else
    return UnknownRole;
} /* конец функции getMyRole() */

/*****
/*
/* Вызов необходимой функции в соответствии с кодом действия кластера.
/* Функция doAction() отделена от функции main() для упрощения
/* примера. Дополнительная информация о действиях кластера приведена в
/* первой части вызываемых функций.
/*
/* Каждый код действия выделен в отдельную функцию только для упрощения
/* данного примера. В конкретной программе выхода некоторые коды функций
/* могут соответствовать одной и той же функции, т.е. различные коды
/* действий обрабатываются одной функцией.
/*
*****/
static int doAction(int actionCode,
                  int role,
                  int priorRole,
                  Qcst_EXTP0100_t *crgData,
                  EpData *epData) {

/*-----*/
/*
/* Выполняется вызов соответствующей функции для обработки
/* кода действия, если он известен этой программе выхода.
/*
/*-----*/

if (actionCode <= MaxAc )
    return (*fcn[actionCode]) (role, priorRole, crgData, epData);
else

/*-----*/
/*

```



```

    /* В новом выпуске операционной системы компания IBM определила новый */
    /* код действия, обработку которого эта программа выхода еще не     */
    /* поддерживает. Выполняется действие по умолчанию.                 */
/*
*/
/*-----*/
    return newActionCode(role, priorRole, crgData, epData);
} /* конец функции doAction() */

/*****
/*
/* Код действия = QcstCrgAcInitialize
/*
/* Вызван API QcstCreateClusterResourceGroup. Создается новый
/* объект группы ресурсов кластера.
/*
/* Замечания:
/* - Проверьте, что программа приложения и все связанные с ней объекты
/* находятся на главном и резервном узлах. Если объектов там нет,
/* возможно, необходимо отправить сообщения об ошибке/предупреждение
/* или вернуть код сбоя действия.
/* - Проверьте, что все необходимые CRG данных и устройств
/* существуют во всех узлах домена восстановления.
/* - Выполните процедуру настройки, необходимую для
/* запуска приложения на основном и резервном узлах.
/* - Если данная CRG позволяет применять API
/* QcstDistributeInformation, то можно создать пользовательскую
/* очередь, необходимую для этого API.
/*
/*****
static int createCrg(int role,
                    int doesNotApply,
                    Qcst_EXTP0100_t *crgData,
                    EpData *epData) {

    return QcstSuccessful;
} /* конец функции createCrg() */

/*****
/*
/* Код действия = QcstCrgAcStart
/*
/* Вызван API QcstStartClusterResourceGroup API. Запускается группа
/* ресурсов кластера.
/* Вызван API QcstInitiateSwitchOver и это второй код действия,
/* передаваемый программе выхода.
/* Произошло событие автоматического переноса
/* ресурсов и это второй код действия, передаваемый программе выхода.
/*
/* Проверка активности всех зависимых CRG выполняется с помощью
/* максимального времени ожидания. Если CRG запущена с помощью API
/* QcstStartClusterResourceGroup, то это время будет малым. В случае
/* принудительного или автоматического переноса ресурсов времени потребуется
/* больше. При выполнении принудительного или автоматического переноса
/* ресурсов CRG данных и устройств становятся доступными не сразу, поэтому
/* время ожидания увеличивается. Ожидание не будет длительным если используется API
/* Запустить CRG, если зависимые CRG уже запущены, если возникли ошибки,
/* в результате которых CRG были запущены неупорядоченно, и т.д.
/*
/* Замечания:
/* - Если это основной узел, то запускается приложение. Эта программа
/* выхода должна вызвать приложение, которое будет выполняться в том же
/* задании или отслеживать все задания, запущенные этой программой
/* выхода, чтобы определить, когда завершается задание приложения.
/* Самый простой способ - вызов и выполнение приложения в этом

```

```

/* задании. */
/* Службы ресурсов кластера не ожидают возврата этой программы */
/* выхода до тех пор, пока не будет завершено выполнение приложения. */
/* - При необходимости запустите связанные подсистемы, серверные задания */
/* и т.д. */
/* - Убедитесь, что необходимые CRG данных активны во всех узлах домена */
/* восстановления. */
/* */
/*****/
static int startCrg(int role,
                   int doesNotApply,
                   Qcst_EXTP0100_t *crgData,
                   EpData *epData) {

    unsigned int maxWaitTime;

    /* Запускает приложение, если этот узел является основным
    if (role == QcstPrimaryNodeRole) {

/*-----*/
/*
/* Определите, все ли CRG, от которых зависит приложение, готовы. */
/* Если проверка дала отрицательный результат, то возвращается код */
/* действия Start. Служба ресурсов кластера изменит состояние CRG на */
/* Inactive. */
/* */
/*-----*/

        if (crgData->Cluster_Resource_Group_Status == QcstCrgStartCrgPending)
maxWaitTime = MaxStartCrgWaitSeconds;
        else
            maxWaitTime = MaxWaitSeconds;
        if (QcstSuccessful != checkDependCrgDataArea(maxWaitTime))
            return QcstSuccessful;

/*-----*/
/*
/* Перед запуском приложения обновляет область данных для */
/* отображения того, что приложение выполняется. */
/* */
/*-----*/

        setApp1CrgDataArea(App1_Running);

/*-----*/
/*
/* Здесь укажите процедуры для вызова приложения. Предполагается, что */
/* управление будет возвращено только в случае завершения приложения: */
/* обычный возврат из программы выхода, отмена задания или возникновение*/
/* необрабатываемой исключительной ситуации. Общие способы отмены задания*/
/* приведены в описании функции cancelHandler(). */
/* */
/*-----*/

/*-----*/
/*
/* После завершения приложения обычным образом обновляет */
/* область данных для отображения того, что приложение больше не */
/* выполняется. */
/* */
/*-----*/

```

```

/*-----*/
    setApp1CrgDataArea(App1_Ended);
}
else

/*-----*/
    /*
    /* Для резервного узла и узла копии отмечает в области
    /* данных, что приложение не выполняется.
    /*
    /*
    /*-----*/
        setApp1CrgDataArea(App1_Ended);

    return QcstSuccessful;
} /* конец функции startCrg() */
/*****
/*
/* Код действия = QcstCrgAcRestart
/*
/* Возникла ошибка в предыдущем вызове программы выхода, вследствие чего для*/
/* кода возврата указано значение QcstFailWithRestart. Или же возникла
/* исключительная ситуация, которой было разрешено отфильтровать стек вызовов.*/
/* В любом случае, максимальное количество разрешенных перезапусков программы*/
/* выхода еще не достигнуто.
/*
/* Этот код действия передается только программам выхода CRG
/* приложений, которые были отменены с помощью кода действия Запустить.
/*
/*****
static int restartCrg(int role,
                    int doesNotApply,
                    Qcst_EXTP0100_t *crgData,
                    EpData *epData) {

/*-----*/
    /*
    /* Выполняет процедуры, необходимые для перезапуска
    /* приложения после сбоя, затем вызывает функцию startCrg() для
    /* выполнения функций запуска.
    /*
    /*-----*/

    return startCrg(role, doesNotApply, crgData, epData);
} /* конец функции restartCrg() */

/*****
/*
/* Код действия = QcstCrgAcEnd
/*
/* Код действия Завершить применяется в одном следующих случаев:
/* - Вызван API QcstEndClusterResourceGroup.
/* - Кластер был разбит на разделы. Этот узел расположен во
/* вспомогательном разделе. Код действия Завершить применяется
/* независимо от, была ли группа CRG активной или неактивной. Кроме
/* того, передаются зависимые данные кода действия
/* QcstPartitionFailure.
/* - Приложение завершено. Кроме того, передаются
/* зависимые данные кода действия QcstResourceEnd. Все узлы из домена
/* восстановления получают один и тот же код действия (включая основной).
/* - Задание CRG отменено. Программа выхода на данном узле будет
/*

```

```

/* вызвана с кодом действия Завершить работу. В качестве кода действия*/
/* зависимых данных будет передано значение QcstMemberFailure. */
/* */
/* */
/* */
/* Замечания: */
/* - Если CRG активна, то задание, управляющее приложением, отменяется */
/* и после отмены программы выхода останавливается устойчивый IP-адрес.*/
/* */
/* - Если задания подсистемы или серверные задания были запущены в */
/* результате кода действия QcstCrgAcStart, их следует завершить */
/* или объединить процедуры для завершения приложения в функции */
/* cancelHandler(), так как она вызывается для всех API служб */
/* ресурсов кластера, которые завершают приложение в текущем */
/* основном узле. */
/* */
/*****
static int endCrg(int role,
                 int priorRole,
                 Qcst_EXTP0100_t *crgData,
                 EpData *epData) {

/*-----*/
/* */
/* Завершает приложение, если оно выполняется в этом узле. */
/* */
/*-----*/
    endApplication(QcstCrgAcRemoveNode, role, priorRole, crgData,
epData);

    return QcstSuccessful;
} /* конец функции endCrg() */

/*****
/* */
/* Код действия = QcstCrgAcVerificationPhase */
/* */
/* Код действия этапа проверки позволяет разрешить программе выхода */
/* выполнить проверку перед дальнейшей обработкой */
/* запрашиваемой функции, заданной с помощью зависимых данных кода */
/* действия. Если программа выхода определяет, что запрашиваемую */
/* функцию обработать невозможно, она должна вернуть */
/* QcstFailWithoutRestart. */
/* */
/* Примечание: Программа выхода не может быть вызвана с помощью кода */
/* действия Отменить. */
/* */
/*****
static int verifyPhase(int role,
                     int doesNotApply,
                     Qcst_EXTP0100_t *crgData,
                     EpData *epData) {

/*-----*/
/* */
/* Выполняется проверка */
/* */
/*-----*/
    if (crgData->Action_Code_Dependent_Data == QcstDltCrg) {
        /* проверка */
        /* если условие не выполняется */

```

```

        /* вернуть QcstFailWithoutRestart */
    }

    return QcstSuccessful;
} /* конец функции verifyPhase() */

/*****
/*
/* Код действия = QcstCrgAcDelete
/*
/* Вызван API QcstDeleteClusterResourceGroup или QcstDeleteCluster.
/* Удаляется группа ресурсов кластера. При этом службы ресурсов кластера
/* активны.
/* В случае применения API QcstDeleteCluster передаются зависимые данные
/* кода действия QcstDltCluster.
/* Если при активной CRG применялся API QcstDeleteCluster, то после
/* обработки кода действия Удалить отменяется задание программы выхода,
/* по-прежнему активное для кода действия Запустить.
/*
/* Замечания:
/* - Удалите прикладные программы и объекты из узлов, в
/* которых они больше не нужны. Например, из резервных узлов.
/* Проявите осторожность при удалении объектов приложений, так как
/* некоторые сценарии могут удалить CRG и оставить объекты
/* приложений во всех узлах.
/*
*****/
static int deleteCrg(int role,
                    int doesNotApply,
                    Qcst_EXTP0100_t *crgData,
                    EpData *epData) {

    return QcstSuccessful;
} /* конец функции deleteCrg() */
/*****
/*
/* Код действия = QcstCrgAcReJoin
/*
/* Могут возникнуть следующие ситуации:
/* 1. Неполадка, в результате которой кластер был разбит на
/* разделы, исправлена и два раздела объединяются в единый кластер.
/* Передаются зависимые данные кода действия QcstMerge.
/* 2. В узле, в котором произошел сбой или который был
/* остановлен, снова запущены службы ресурсов кластера и он
/* добавляется в кластер. Передаются зависимые данные кода действия
/* QcstJoin.
/* 3. Перезапущено задание CRG в конкретном узле, которое было отменено
/* или завершено. Передаются зависимые данные кода действия QcstJoin.
/*
/*
/* Замечания:
/* - Если приложение копирует информацию о состоянии приложения в другие
/* узлы и если CRG активен, то при выполнении приложения эту информацию
/* потребуется повторно синхронизировать в добавляемых узлах.
/* - Проверьте отсутствующие объекты приложений в добавляемых узлах.
/* - Убедитесь, что в добавляемых узлах присутствуют необходимые
/* CRG данных.
/* - Если CRG приложения активен, убедитесь, что активны необходимые CRG
/* данных.
/*
*****/
static int memberIsJoining(int role,
                          int priorRole,
                          Qcst_EXTP0100_t *crgData,
                          EpData *epData) {

```

```

/*-----*/
/*
/* Если данный узел не является основным, позволяет указать в
/* области данных, что приложение не выполняется.
*/
/*
/*-----*/
if (role != QcstPrimaryNodeRole) {
    setApp1CrgDataArea(App1_Ended);
}

/*-----*/
/*
/* Если в кластер добавляется один узел, то для выполнения доступен
/* определенный набор действий. В случае объединения узлов кластера,
/* который был разбит на разделы, может быть доступен другой
/* набор действий.
*/
/*
/*-----*/
if (crgData->Action_Code_Dependent_Data == QcstJoin) {
    /* Действия для добавления узла в кластер
*/
}
else {
    /* Действия для объединения разделов
*/
}

return QcstSuccessful;
} /* конец функции memberIsJoining()
*/

/*****/
/*
/* Код действия = QcstCrgAcFailover
*/
/*
/* Для этой группы ресурсов кластера в конкретном узле
*/
/* или нескольких узлах произошел сбой служб ресурсов кластера или
*/
/* их работа была завершена. Код действия Автоматический перенос
*/
/* ресурсов передается независимо от того, был CRG активен или нет.
*/
/* Автоматический перенос ресурсов может произойти в следующих
*/
/* случаях:
*/
/*
/* - оператор отменил задание CRG на узле. Передаются зависимые данные
*/
/* кода действия QcstMemberFailure.
*/
/* - Завершена работа служб ресурсов кластера (например,
*/
/* завершена подсистема QSYSWRK, пока CRS был активен). Передаются
*/
/* зависимые данные кода действия QcstNodeFailure.
*/
/* - Произошел сбой приложения для CRG приложений в основном
*/
/* узле, в результате которого это приложение не удалось перезапустить.
*/
/* CRG активен. Передаются зависимые данные кода
*/
/* действия QcstApp1Failure.
*/
/* - Произошел сбой узла (например, сбой питания). Передаются зависимые
*/
/* данные кода действия QcstNodeFailure.
*/
/* - Кластер распался вследствие сбоя связи, например, сбой линии связи
*/
/* или локальной сети. Код действия Автоматический перенос ресурсов
*/
/* передается узлам домена восстановления большинства разделов.
*/
/* Узлам меньшинства разделов передается код действия Завершить работу.
*/
/* Будут переданы зависимые данные кода действия QcstPartitionFailure.
*/
/* - Работа узла в домене восстановления CRG завершается с помощью
*/
/* API QcstEndClusterNode. Этот узел получает код действия Завершить
*/
/* узел. Все остальные узлы домена восстановления получают код действия
*/
/* Автоматический перенос ресурсов. Для этого кода действия передаются
*/
/* зависимые данные кода действия QcstEndNode.
*/
/* - Активный узел домена восстановления для активной CRG удаляется из
*/
/* кластера посредством API QcstRemoveClusterNodeEntry.
*/
*/

```

```

/* Будут передаваться зависимые данные кода действия QcstRemoveNode. */
/* Если для активной CRG удалится неактивный узел, или если сама CRG */
/* неактивна, то передается код действия Удалить узел. */
/* */
/* Программа выхода вызывается независимо от того, активен CRG */
/* или нет. Если CRG неактивен, то для программы выхода могут */
/* отсутствовать доступные действия. */
/* */
/* Если CRG активен и оставшийся элемент был основным узлом, */
/* выполните функции, необходимые для автоматического */
/* переноса ресурсов и создания нового основного узла. */
/* */
/* Поле Action_Code_Dependent_Data позволяет определить, если */
/* - сбой произошел в результате неполадки, вследствие которой кластер */
/* был разбит на разделы (изменяются все CRG, для которых в домене */
/* восстановления существовали разделенные узлы) */
/* - произошел сбой узла или в узле завершилась работа служб ресурсов */
/* кластера (изменяются все CRG, для которых в домене восстановления */
/* существовал узел, работа которого была завершена или в ней */
/* произошел сбой) */
/* - изменена только одна CRG (например, в узле было отменено одно задание */
/* CRG или же возникла ошибка в одном приложении) */
/* */
/* */
/* Замечания: */
/* - Подготовьте новый основной узел для запуска приложения. */
/* - Запускать приложение в данный момент НЕ рекомендуется. Программа */
/* выхода будет вновь вызвана с кодом действия QcstCrgAcStart, если */
/* CRG была активна при сбое. */
/* - Если CRG приложения активен, убедитесь, что активны необходимые CRG */
/* данных. */
/* */
/*****/
static int memberIsLeaving(int role,
                          int priorRole,
                          Qcst_EXTP0100_t *crgData,
                          EpData *epData) {

/*-----*/
/* */
/* Если CRG активен, выполняется автоматический перенос */
/* ресурсов. В противном случае действия не выполняются. */
/* */
/*-----*/
if (crgData->Original_Cluster_Res_Grp_Stat == QcstCrgActive) {

/*-----*/
/* */
/* CRG активен. Определяется, изменилась ли роль данного узла и */
/* является ли он новым основным узлом. */
/* */
/*-----*/

if (priorRole != role && role == QcstPrimaryNodeRole) {

/*-----*/
/* */
/* Данный узел стал основным узлом. Выполняются действия по */
/* автоматическому переносу ресурсов, так эта программа */
/* выхода будет снова вызвана с кодом действия Запустить. */
/* */
/*-----*/

```

```

/*-----*/

/*-----*/
/*
/* Указывает в области данных этого узла, что приложение не */
/* выполняется. */
*/
/*-----*/
    setApplCrgDataArea(Appl_Ended);

/*-----*/
/*
/* Если приложение не выполняет действий с кодом Запустить */
/* и станет активным только после активации устойчивого IP-адреса, */
/* то следующие строки необходимо раскомментировать. В них определя-*/
/* ется, все ли CRG, от которых зависит приложение, готовы. */
/* Если проверка дала отрицательный результат, то возвращается */
/* сбой кода действия. */
*/
/*-----*/

/*
/* if (QcstSuccessful != checkDependCrgDataArea(MaxWaitSeconds)) */
/* return QcstFailWithOutRestart; */
*/
}
}

return QcstSuccessful;
} /* конец функции memberIsLeaving() */

/*****/
/*
/* Код действия = QcstCrgAcSwitchover */
/*
/* Вызван API QcstInitiateSwitchover. Первый резервный узел из домена */
/* восстановления группы ресурсов кластера становится основным узлом, а */
/* текущий основной узел становится последним резервным узлом. */
/*
/* Замечания: */
/* - Подготовьте новый основной узел для запуска приложения. */
/* - Запускать приложение в данный момент НЕ рекомендуется. Программа выхода */
/* будет вызвана с кодом действия QcstCrgAcStart. */
/* - Если CRG активна и узел является основным, то после вызова */
/* задание, управляющее приложением, и завершается устойчивый IP-адрес.*/
/*
/* - Убедитесь, что перенесены и активны необходимые CRG */
/* данных или устройств. */
/*
/*****/
static int switchPrimary(int role,
                        int priorRole,
                        Qcst_EXTP0100_t *crgData,
                        EpData *epData) {

/*-----*/
/*
/* Проверяется, является ли текущий узел прежним основным узлом. */
*/
/*-----*/
    if (priorRole == QcstPrimaryNodeRole) {

```



```

/*-----*/
/*
/* Перед переносом выполните необходимые действия по очистке прежнего */
/* основного узла. Не забудьте, что задание, управлявшее программой */
/* выхода, которая запустила приложение, уже отменено. */
/*
/* Например, можно очистить все процессы, блокирующие базу данных. */
/* Для этого необходимо вызвать программу обработки отмены приложения. */
/*-----*/
}

/*-----*/
/*
/* Текущий узел не является прежним основным. Проверяется, является ли */
/* он новым основным узлом. */
/*
/*-----*/

else if (role == QcstPrimaryNodeRole) {

/*-----*/
/*
/* Выполните действия над новым основным узлом, необходимые перед */
/* запуском приложения с кодом действия QcstCrgAcStart. */
/*
/*-----*/

/*-----*/
/*
/* Позволяет указать в области данных этого узла, что приложение не */
/* выполняется. */
/*
/*-----*/
setApp1CrgDataArea(App1_Ended);

/*-----*/
/*
/* Если приложение не выполняет действий с кодом Запустить */
/* и станет активным только после активации устойчивого IP-адреса, */
/* то следующие строки необходимо раскомментировать. В них определя- */
/* ется, все ли CRG, от которых зависит приложение, готовы. */
/* Если проверка дала отрицательный результат, то возвращается */
/* сбой кода действия. */
/*
/*-----*/
/*
/* if (QcstSuccessful != checkDependCrgDataArea(MaxWaitSeconds)) */
/* return QcstFailWithOutRestart; */
/*
/*
/*-----*/
}
else {

/*-----*/
/*
/* Данный узел является резервным узлом или узлом-копией. */
/* Если для этих узлов предусмотрены действия, то укажите их здесь. */
/* Если нет, то этот блок else можно удалить. */
/*
/*-----*/

/*-----*/

/*-----*/
}
}

```

```

    /*
    /* Позволяет указать в области данных этого узла, что приложение не
    /* выполняется.
    /*
    /*-----*/
    setApp1CrgDataArea(App1_Ended);
    }

    return QcstSuccessful;
} /* конец функции switchPrimary() */

/*****
/*
/* Код действия = QcstCrgAcAddNode
/*
/* Вызван API QcstAddNodeToRcvyDomain. В домен восстановления группы
/* ресурсов кластера добавляется новый узел.
/*
/* Замечания:
/* - В домен восстановления добавляется новый узел. См. замечания,
/* приведенные для функции createCrg().
/* - Если данная CRG позволяет применять API
/* QcstDistributeInformation, то можно создать пользовательскую
/* очередь, необходимую для этого API.
/*
*****/
static int addNode(int role,
                  int priorRole,
                  Qcst_EXTP0100_t *crgData,
                  EpData *epData) {

/*-----*/

    /*
    /* Определяется, является ли текущий узел добавляемым узлом.
    /*
    /*-----*/

    if (0 == memcmp(&crgData->This_Nodes_ID,
                   &crgData->Changing_Node_ID,
                   sizeof(Qcst_Node_Id_t)))
    {

/*-----*/

        /*
        /* Задает состояние области данных нового узла.
        /*
        /*-----*/

        setApp1CrgDataArea(App1_Ended);

/*-----*/

        /*
        /* Создает очередь, необходимую для API распространения информации.
        /*
        /*-----*/

        if (0 == memcmp(&crgData->DI_Queue_Name,
                       Nulls,
                       sizeof(crgData->DI_Queue_Name)))

```

```

    {
    }
}

return QcstSuccessful;
} /* конец функции addNode() */
/*****
/*
/* Код действия = QcstCrgAcRemoveNode */
/*
/* Вызван API QcstRemoveNodeFromRcvyDomain или */
/* QcstRemoveClusterNodeEntry. Узел удаляется из домена */
/* восстановления группы ресурсов кластера или он полностью */
/* удаляется из кластера. */
/*
/* Код действия получается следующими элементами: */
/* Для API QcstRemoveClusterNodeEntry: */
/* - Если удаленный узел активен, а CRG неактивна, то этот код действия */
/* получают все узлы домена восстановления, включая удаляемый узел. */
/* Узлы, которые не удаляются, получают зависимые данные кода действия*/
/* QcstNodeFailure. */
/* - Если удаленный узел активен и активна CRG, то удаляемый */
/* узел получает код действия Удалить узел. Все остальные узлы */
/* домена восстановления получают код действия */
/* Автоматический перенос ресурсов и зависимые данные кода действия */
/* QcstNodeFailure. */
/* - Если удаляемый узел неактивен в кластере, все узлы домена */
/* восстановления получают этот код действия. */
/* Для API QcstRemoveNodeFromRcvyDomain: */
/* - Все узлы получают код действия Удалить узел независимо */
/* от того, активен CRG или нет. Кроме того передаются зависимые */
/* данные кода действия QcstRmvRcvyDmnNode. */
/*
/* Замечания: */
/* - Вы можете очистить удаленный узел. Для необходимо удалить */
/* ненужные объекты. */
/* - Если CRG активна и узел является основным, то после вызова */
/* программы выхода отменяется задание, управляющее приложением, и */
/* завершается устойчивый IP-адрес. */
/* - Если задания подсистемы или серверные задания были запущены в */
/* результате кода действия QcstCrgAcStart, их следует завершить */
/* или объединить процедуры для завершения приложения в функции */
/* cancelHandler(), так как она вызывается для всех API служб */
/* ресурсов кластера, которые завершают приложение в текущем */
/* основном узле. */
/*
/*****
static int rmvNode(int role,
                  int priorRole,
                  Qcst_EXTP0100_t *crgData,
                  EpData *epData) {

/*-----*/

/*
/* Определяется, является ли текущий узел удаляемым узлом.
/*
/*-----*/

if (0 == memcmp(&crgData->This_Nodes_ID,
               &crgData->Changing_Node_ID,
               sizeof(Qcst_Node_Id_t)))
{

/*-----*/

```

```

        /*
        /* Завершает приложение, если оно выполняется в этом узле.
    /*
    /*-----*/
        endApplication(QcstCrgAcRemoveNode, role, priorRole, crgData,
epData);

    }
    return QcstSuccessful;
} /* конец функции rmvNode()

/*****
/*
/* Код действия = QcstCrgAcChange
/*
/* Вызван API QcstChangeClusterResourceGroup. Изменяется информация или
/* атрибуты, хранящиеся в объекте группы ресурсов кластера. Обратите
/* внимание, что программа выхода вызывается не для всех изменений
/* объекта CRG. Начиная с выпуска V5R1M0, программа выхода вызывается
/* только в следующих случаях
/* - изменяется текущий домен восстановления
/* - изменяется предпочитаемый домен восстановления
/*
/* Если вносятся указанные изменения и для программы выхода
/* задается значение *NONE, то программа выхода не вызывается.
/*
/* Замечания:
/* - Информацию и процессы этой группы ресурсов домена можно изменить
/* только в том случае, если вносятся изменения в домен восстановления.
/* Обратите внимание, что если активен CRG, то основной узел нельзя
/* изменить с помощью API QcstChangeClusterResourceGroup.
/*
/*****
static int chgCrg(int role,
                int priorRole,
                Qcst_EXTP0100_t *crgData,
                EpData *epData) {

    return QcstSuccessful;
} /* конец функции chgCrg()

/*****
/*
/* Код действия = QcstCrgAcDeleteCommand
/*
/* Для удаления объекта группы ресурсов кластера вызвана команда CL
/* Удалить группу ресурсов кластера (DLTCRG). При этом вызван
/* API QcstDeleteCluster или API QcstRemoveClusterNodeEntry.
/* В обоих случаях службы ресурсов кластера неактивны в узле, в котором,
/* вызвана команда или API. Таким образом, действие этой функции не
/* распространяется на весь кластер, а ограничено узлом, в котором вызвана
/* команда CL или API.
/*
/* В случае применения API QcstDeleteCluster передаются зависимые данные
/* кода действия QcstDltCluster.
/*
/* См. замечания, приведенные для функции deleteCrg()
/*
/*****
static int deleteCrgWithCmd(int role,
                          int doesNotApply,
                          Qcst_EXTP0100_t *crgData,
                          EpData *epData) {

```

```

return QcstSuccessful;
} /* конец функции deleteCrgWithCmd() */

/*****
/*
/* Код действия = QcstCrgEndNode
/*
/* Вызван API QcstEndClusterNode или отменено задание CRG.
/*
/*
/* Код действия QcstCrgEndNode передается программе выхода только в том
/* узле, который завершается или в котором было отменено задание CRG. В узел, где отменено задание */
/* службы ресурсов кластера, передаются зависимые данные кода
/* действия QcstMemberFailure.
/*
/* Завершение работы службы ресурсов кластера на этом узле или завершение
/* задания CRG приведет к автоматическому переносу ресурсов во всех
/* остальных узлах кластера. Этим узлам будут переданы зависимые данные
/* кода действия QcstCrgAcFailover. В случае отмены задания будут переданы
/* зависимые данные кода QcstMemberFailure, а в случае завершения работы
/* узла - код QcstNodeFailure.
/*
/*
/* Замечания:
/* - Если CRG активна и узел является основным, то после вызова
/* программы выхода отменяется задание, управляющее приложением, и
/* завершается устойчивый IP-адрес.
/* - Если задания подсистемы или серверные задания были запущены в
/* результате кода действия QcstCrgAcStart, их следует завершить здесь.
/*
/*****
static int endNode(int role,
                  int priorRole,
                  Qcst_EXTP0100_t *crgData,
                  EpData *epData) {

/*-----*/
/*
/* Завершает приложение, если оно выполняется в этом узле.
/*
/*-----*/
endApplication(QcstCrgEndNode, role, priorRole, crgData, epData);

return QcstSuccessful;
} /* конец функции endNode() */

/*****
/*
/* Код действия = QcstCrgAcChgNodeStatus
/*
/* Вызван API QcstChangeClusterNodeEntry. Данный API позволяет
/* сообщить службам ресурсов кластера о том, что этот узел не был
/* разбит на разделы, а в нем произошел сбой.
/*
/*
/* Замечания:
/* - Перед этим была вызвана программа выхода с кодом действия
/* QcstCrgAcEnd при активной CRG, или с кодом действия
/* QcstCrgAcFailover при неактивной CRG, поскольку служба ресурсов
/* кластера предполагала, что кластер распался. Теперь пользователь
/* сообщает службе ресурсов кластера о том, что на самом деле в узле
/* произошел сбой. Программа выхода может выполнить действия только
/* в том случае, если до получения подтверждения узла выполнялись
/* какие-либо действия, которые теперь необходимо отменить.
/*
/*****
static int chgNodeStatus(int role,

```

```

        int priorRole,
        Qcst_EXTP0100_t *crgData,
        EpData *epData) {

    return QcstSuccessful;
} /* конец функции chgNodeStatus() */

/*****
/*
/* Код действия = QcstCrgAcCancelFailover
/*
/* В основном узле произошел сбой или завершена работа служб
/* ресурсов кластера этой группы ресурсов кластера.
/* В очередь сообщений автоматического переноса
/* ресурсов, указанную для этого CRG, отправлено сообщение, в
/* результате которого восстановление после сбоя было отменено.
/* При этом состояние CRG будет изменено на неактивное, текущий
/* основной узел останется основным.
/*
/* Замечания:
/* - Основной узел больше не участвует в операциях кластера. Неполадка,
/* которая привела к сбою основного узла должна быть устранена для
/* того, чтобы снова запустить CRG.
/*
*****/
static int cancelFailover(int role,
        int priorRole,
        Qcst_EXTP0100_t *crgData,
        EpData *epData) {

    return QcstSuccessful;
} /* конец функции cancelFailover() */

/*****
/*
/* Код действия = программа выхода его еще не знает
/*
/* Программа выхода получила новый код действия. Это может произойти
/* установки нового выпуска i5/OS в случае вызова нового API кластера
/* или появления нового события кластера. Программа выхода еще не была
/* обновлена для поддержки нового кода действия.
/*
/* Для обработки новых кодов действий можно применять две
/* различные стратегии. Выбор правильной стратегии зависит от
/* действий, выполняемых этой программой выхода для приложения.
/*
/* Первая стратегия заключается в следующем: действия не выполняются и
/* возвращается успешный код возврата.
/* Такой подход позволяет полностью выполнить API кластера или событие. */
/* Функция будет выполнена успешно даже в том случае, если эта программа
/* выхода не поддерживает новый код действия. При этом возникает риск
/* невыполнения предусмотренного действия. В таких случаях рекомендуется
/* заносить в протокол сообщения об ошибках, чтобы впоследствии можно
/* было определить их причины и обновить программу выхода.
/*
/* Другой вариант - вернуть код ошибки, например,
/* QcstFailWithRestart. Это означает, что новый API кластера
/* нельзя будет применить до тех пор, пока программа выхода не получит
/* новый код действия. В таких случаях также рекомендуется заносить
/* в протокол сообщение об ошибке, чтобы потом определить ее причину.
/*
/* Выбрать наиболее подходящий подход может только разработчик
/* программы выхода.
/*
*****/

```

```

static int newActionCode(int role,
                        int doesNotApply,
                        Qcst_EXTP0100_t *crgData,
                        EpData *epData) {

/*-----*/
/*
/* Добавьте процедуры для занесения в протокол сообщения об ошибке
/* (очередь сообщений оператора, протокол задания, протокол ошибок
/* приложения и т.д.). Это позволит вовремя обновлять программу
/* выхода для обработки новых кодов действий.
*/
/*
/* Обратите внимание, что по умолчанию применяется описанная
/* выше стратегия, в результате которой действия не выполняются.
*/
/*
/*-----*/

return QcstSuccessful;
} /* конец функции newActionCode() */

/*****
/*
/* Код действия = QcstCrgAcUndo
*/
/*
/* Примечание: Программу выхода нельзя вызывать с кодом действия Отменить,
/* если до этого выполнялось действие с одним из следующих кодов:
/* QcstCrgAcChgNodeStatus
/* QcstCrgAcDelete
/* QcstCrgAcDeleteCommand
/* QcstCrgAcEndNode
/* QcstCrgAcRemoveNode (Если из кластера удаляется активный узел
/* и применяется API Удалить узел кластера.
/* Если из кластера удаляется неактивный узел,
/* то действие Отменить можно вызвать с API Удалить
/* узел из домена восстановления и Удалить узел
/* кластера.
/* QcstCrgAcRestart
/* QcstCrgAcUndo
*/
/*
/* В работе API, которые могут вызывать программы выхода, предусмотрены
/* три этапа.
/* 1. Выполняются процедуры, которые необходимо выполнить перед
/* тем, как вызвать программу выхода.
/* 2. Вызывается программы выхода.
/* 3. Выполняются процедуры, которые необходимо выполнить после
/* вызова программы выхода.
*/
/*
/* Ошибки, возникшие на этапах 2 и 3, учитываются при повторном
/* вызове программы выхода с кодом действия Отменить. При таком подходе
/* программа выхода может откатить все действия, выполненные при первом
/* вызове API. Кроме того, API также откатит действия, выполненные
/* при попытке возврата состояния кластера и объектов кластера,
/* в котором они находились до вызова API.
*/
/*
/* Предполагается, что в ответ на указанный код действия возвращаются
/* следующие коды возврата, так как от этого зависит, какое действие будет
/* выполнено.
*/
/*
/* QcstCrgAcInitialize: QcstSuccessful; CRG не создается.
/* QcstCrgAcStart: QcstSuccessful; CRG не запускается
/* QcstCrgAcEnd: QcstFailWithOutRestart; CRG переходит в состояние
/* Под вопросом. Необходимо
/* определить причину сбоя.
/* QcstCrgAcReJoin: QcstFailWithOutRestart; CRG переходит в состояние

```

```

/*          Под вопросом. Необходимо */
/*          определить причину сбоя. */
/* QcstCrgAcFailover: QcstFailWithOutRestart; CRG переходит в состояние*/
/*          Под вопросом. Необходимо */
/*          определить причину сбоя. */
/* QcstCrgAcSwitchover: QcstFailWithOutRestart; CRG переходит в состояние*/
/*          Под вопросом. Необходимо */
/*          определить причину сбоя. */
/* QcstCrgAcAddNode: QcstSuccessful; Узел не добавляется */
/* QcstCrgAcRemoveNode: QcstFailWithOutRestart; CRG переходит в состояние*/
/*          Под вопросом. Необходимо */
/*          определить причину сбоя. */
/* QcstCrgAcChange: QcstSuccessful; Домен восстановления не */
/* изменен. */
/*
/*****
static int undoPriorAction(int role,
                          int priorRole,
                          Qcst_EXTP0100_t *crgData,
                          EpData *epData) {

/*-----*/
/*
/* Предыдущий код действия определяет действия программы выхода в случаях*/
/* сбоя, отмены и получения безуспешного кода возврата. */
/*
/*-----*/
    if (crgData->Prior_Action_Code <= MaxAc )
        return (*undoFcn[crgData-&lt;Prior_Action_Code]
                (role, priorRole, crgData,
epData);
    else

/*-----*/
/*
/* В новом выпуске операционной системы компания IBM определила новый */
/* код действия, обработку которого эта программа выхода еще не */
/* поддерживает. Выполняется действие по умолчанию. */
/*
/*-----*/
    return newActionCode(role, priorRole, crgData, epData);
} /* конец функции undoPriorAction()

/*****
/*
/* Код действия = QcstCrgAcUndo */
/*
/* Предыдущий код действия = QcstCrgAcInitialize */
/*
/* Замечания: */
/* CRG не создается. Объекты, которые могли быть созданы в узлах */
/* домена восстановления, должны быть удалены, так как если они */
/* будут существовать, то последующая попытка их создания может */
/* быть не выполнена. */
/*
/*****
static int undoCreateCrg(int role,
                        int doesNotApply,
                        Qcst_EXTP0100_t *crgData,
                        EpData *epData) {

    return QcstSuccessful;
} /* конец функции undoCreateCrg()

```



```

/*****/
/*                                                                 */
/* Код действия = QcstCrgAcUndo                                   */
/*                                                                 */
/* Предыдущий код действия = QcstCrgAcStart                       */
/*                                                                 */
/* Замечания:                                                    */
/* Произошел сбой службы ресурсов кластеров при завершении API Запустить */
/* CRG после вызова программы выхода с кодом действия Запустить.  */
/*                                                                 */
/* На основном узле будет отменено задание программы выхода, управляющее */
/* приложением. Затем программа выхода будет вызвана с кодом действия */
/* Отменить.                                                       */
/*                                                                 */
/* Все остальные узлы домена восстановления будут вызваны с кодом */
/* действия Отменить.                                             */
/*                                                                 */
/*****/
static int undoStartCrg(int role,
                        int doesNotApply,
                        Qcst_EXTP0100_t *crgData,
                        EpData *epData) {

    return QcstSuccessful;
} /* конец функции undoStartCrg() */

/*****/
/*                                                                 */
/* Код действия = QcstCrgAcUndo                                   */
/*                                                                 */
/* Предыдущий код действия = QcstCrgAcEnd                         */
/*                                                                 */
/* Замечания:                                                    */
/* CRG не завершается. Если программа выхода выполнила действия по */
/* завершению работы приложения, то она может перезапустить приложение */
/* или принять решение о нецелесообразности перезапуска. Если приложение*/
/* не перезапускается, то код возврата должен быть равен QcstFailWithOutRestart, */
/* чтобы CRG можно было перевести в состояние Под вопросом.     */
/*                                                                 */
/*****/
static int undoEndCrg(int role,
                      int doesNotApply,
                      Qcst_EXTP0100_t *crgData,
                      EpData *epData) {

    return QcstFailWithOutRestart;
} /* конец функции undoEndCrg() */

/*****/
/*                                                                 */
/* Код действия = QcstCrgAcUndo                                   */
/*                                                                 */
/* Предыдущий код действия = QcstCrgAcReJoin                     */
/*                                                                 */
/* Замечания:                                                    */
/* Произошла ошибка, которая не позволит добавить компонент в эту группу */
/* CRG. Необходимо проверить все действия, выполненные при получении */
/* кода действия Добавить, и определить те из них, которые следует */
/* отменить, если этот элемент не является активным элементом группы CRG.*/
/*                                                                 */
/*****/
static int undoMemberIsJoining(int role,
                               int doesNotApply,

```

```

        Qcst_EXTP0100_t *crgData,
        EpData *epData) {

    return QcstFailWithOutRestart;
} /* конец функции undoMemberIsJoining() */

/*****
/*
/* Код действия = QcstCrgAcUndo
/*
/* Предыдущий код действия = QcstCrgAcFailover
/*
/* Замечания:
/* Это не означает, что сбой узла или компонента отменен. Также это не
/* означает необратимость сбоя. Это означает ошибку программы выхода при
/* обработке кода действия Автоматический перенос ресурсов. Также после
/* кластера при вызове программы выхода.
/* Если CRG была активной в процессе автоматического*/
/* переноса ресурсов, то не в этом участке. Устойчивый ресурс завершает
/* работу и ожидает вмешательства пользователя. После устранения неполадки
/* следует запустить CRG с помощью API Запустить CRG.
/*
/*
/*****
static int undoMemberIsLeaving(int role,
                               int doesNotApply,
                               Qcst_EXTP0100_t *crgData,
                               EpData *epData) {

    return QcstFailWithOutRestart;
} /* конец функции undoMemberIsLeaving() */

/*****
/*
/* Код действия = QcstCrgAcUndo
/*
/* Предыдущий код действия = QcstCrgAcSwitchover
/*
/* Замечания:
/* Возникла ошибка в процессе перемещения точки доступа из
/* исходного основного узла в новый основной узел.
/* До перемещения точки доступа IP-адрес в исходном основном узле был
/* завершен и снова запущен в этом же узле. Теперь служба ресурсов
/* кластера пытается вернуть точку доступа обратно в исходный основной
/* узел. Программа выхода приложения и устойчивый IP-адрес
/* будут снова запущены в исходном основном узле.
/*
/*
/*****
static int undoSwitchPrimary(int role,
                             int doesNotApply,
                             Qcst_EXTP0100_t *crgData,
                             EpData *epData) {

    return QcstFailWithOutRestart;
} /* конец функции undoSwitchPrimary() */

/*****
/*
/* Код действия = QcstCrgAcUndo
/*
/* Предыдущий код действия = QcstCrgAcAddNode
/*
/* Замечания:

```

```

/* Если объекты были созданы в новом узле, их следует удалить */
/* для того, чтобы впоследствии можно было выполнить команду */
/* Добавить узел в домен восстановления. */
/* */
/* */
/*****/
static int undoAddNode(int role,
                      int doesNotApply,
                      Qcst_EXTP0100_t *crgData,
                      EpData *epData) {

    return QcstSuccessful;
} /* конец функции undoAddNode() */

/*****/
/* */
/* Код действия = QcstCrgAcUndo */
/* */
/* Предыдущий код действия = QcstCrgAcRemoveNode */
/* */
/* Замечания: */
/* Узел все еще находится в домене восстановления. Если объекты были */
/* удалены из узла, их следует снова добавить в него. */
/* */
/*****/
static int undoRmvNode(int role,
                      int doesNotApply,
                      Qcst_EXTP0100_t *crgData,
                      EpData *epData) {

    return QcstFailWithOutRestart;
} /* конец функции undoRmvNode() */

/*****/
/* */
/* Код действия = QcstCrgAcUndo */
/* */
/* Предыдущий код действия = QcstCrgAcChange */
/* */
/* Замечания: */
/* Изменения, внесенные в CRG, будут отменены для того, чтобы */
/* восстановить состояние CRG и домена восстановления, в */
/* котором они находились до попытки изменения. Изменения, */
/* внесенные программой выхода, также должны быть отменены. */
/* */
/*****/
static int undoChgCrg(int role,
                     int doesNotApply,
                     Qcst_EXTP0100_t *crgData,
                     EpData *epData) {

    return QcstSuccessful;
} /* конец функции undoChgCrg() */

/*****/
/* */
/* Код действия = QcstCrgAcUndo */
/* */
/* Предыдущий код действия = QcstCrgAcCancelFailover */
/* */
/* Замечания: */
/* Это не означает, что сбой узла или компонента отменен. Также это не */
/* означает необратимость сбоя. Это означает ошибку службы ресурсов */
/* кластера при вызове программы выхода. */
/* CRG будет находиться в состоянии Под вопросом независимо от того, */

```

```

/* что вернет программа выхода. В данном случае требуется вмешательств */
/* пользователя. После устранения неполадки следует запустить CRG */
/* с помощью API Запустить CRG. */
/* */
/* */
/*****/
static int undoCancelFailover(int role,
                              int doesNotApply,
                              Qcst_EXTP0100_t *crgData,
                              EpData *epData) {

    return QcstSuccessful;
} /* конец функции undoCancelFailover() */

/*****/
/* */
/* Простая процедура, позволяющая из имени объекта и имени библиотеки, */
/* оканчивающихся символом NULL, создать 20-символьное полное имя, не */
/* оканчивающееся символом NULL. */
/* */
/*****/
static void bldDataAreaName(char *objName, char* libName, char *qualName) {

    memset(qualName, 0x40, 20);
    memcpy(qualName, objName, strlen(objName));
    qualName += 10;
    memcpy(qualName, libName, strlen(libName));
    return;
} /* конец функции bldDataAreaName() */

/*****/
/* */
/* В области данных проверяется готовность всех CRG, связанных с данным */
/* приложением. Если готовности нет, то программа через некоторое время */
/* повторяет проверку. */
/* Этот процесс продолжается до тех пор, пока не будут готовы все */
/* зависимые CRG или пока не истечет максимальное разрешенное время */
/* ожидания. Время ожидания можно изменить, если это целесообразно */
/* для конкретной ситуации. */
/* */
/* */
/*****/
static int checkDependCrgDataArea(unsigned int maxWaitTime) {

    Qus_EC_t errCode = { sizeof(Qus_EC_t), 0 };
    char dataAreaName[20];
    struct {
        Qwc_Rdtaa_Data_Returned_t stuff;
        char ready;
    } data;

    /*-----*/
    /* */
    /* Это общее время ожидания готовности зависимых CRG. */
    /* */
    /*-----*/
    unsigned int timeWaited = 0;

    /*-----*/
    /* */
    /* Определение времени ожидания. */
    /* */
    /*-----*/

```

```

/*-----*/
    _MI_Time    timeToWait;
    int hours   = 0;
    int minutes = 0;
    int seconds = WaitSecondsIncrement;
    int hundreths = 0;
    short int options = _WAIT_NORMAL;
    mitime( &timeToWait, hours, minutes, seconds, hundreths );

/*-----*/
    /*
    /* Создается полное имя области данных.
    /*
/*-----*/

    bldDataAreaName(DependCrgDataArea, ApplLib, dataAreaName);

/*-----*/
    /*
    /* Из области данных загружается информация о готовности всех CRG. Если
    /* приложение может продолжить работу, эта область данных обновляется с
    /* помощью партнеров по разработке приложений высокой готовности.
    /*
/*-----*/

    QWCRDTAA(&data,
             sizeof(data),
             dataAreaName,
             offsetof(Qcst_HAAPP0_t,Data_Status)+1, /* API необходим 1 источник */
             sizeof(data.ready),
             &errCode);

/*-----*/
    /*
    /* Если зависимые CRG не готовы, программа ожидает в течение заданного
    /* времени, затем снова выполняет проверку.
    /*
/*-----*/

    while (data.ready != Data_Available) {

/*-----*/
        /*
        /* Если зависимые CRG не будут готовы по истечению максимального
        /* времени ожидания, будет возвращена ошибка. Рекомендуется внести
        /* в протокол сообщение с описанием того, почему приложение не
        /* запустилось, чтобы можно было разобраться в причинах неполадки.
        /*
/*-----*/

        if (timeWaited >= maxWaitTime)
            return QcstFailWithOutRestart;

/*-----*/
        /*
        /* Позволяет дождаться готовности CRG.
        /*
/*-----*/

        waittime(&timeToWait, options);
        timeWaited += WaitSecondsIncrement;

```

```

/*-----*/
/*
/* Из области данных снова загружается информация о готовности CRG. */
/*
/*-----*/
    QWCRDTAA(&data,
            sizeof(data),
            dataAreaName,
            offsetof(Qcst_HAAPPO_t,Data_Status)+1, /* API необходим 1 источник */
            sizeof(data.ready),
            &errCode);
}

return QcstSuccessful;
} /* конец функции checkDependCrgDataArea() */

/*****
/*
/* Обновляется область данных CRG приложения. При этом в ней отображается,
/* что приложение выполняется или не выполняется. Информация из этой
/* области данных применяется партнерами по разработке приложений высокой
/* готовности для координации операций принудительного переноса
/* ресурсов между CRG, зависимыми друг от друга.
/*
/*-----*/
static void setApp1CrgDataArea(char status) {

    char cmd[54];
    char cmdEnd[3] = {0x00, '}', 0x00};

/*-----*/
/*
/* Создается командная строка CL с именем библиотеки области
/* данных, именем области данных, а также символом для записи в
/* область данных. Затем выполняется команда CL.
/*
/*-----*/
    memcpy(cmd, "CHGDTAARA DTAARA(", strlen("CHGDTAARA DTAARA")+1);
    strcat(cmd, App1Lib);
    strcat(cmd, "/");
    strcat(cmd, App1CrgDataArea);
    strcat(cmd, " (425 1)) VALUE("); /* @A1C */
    cmdEnd[0] = status;
    strcat(cmd, cmdEnd);

    system(cmd);

    return;
} /* конец функции setApp1CrgDataArea() */

/*****
/*
/* Эта функция вызывается всякий раз когда программа получает исключительную
/* ситуацию, которая не отслеживается обработчиком исключительных ситуаций. Укажите
/* здесь соответствующие процедуры очистки.
/* При этом задается код возврата сбой и управление передается операционной
/* системе. Задание, управляющее этой программой выхода, завершается.
/*
/* Если исключительная ситуация произошла до определения роли
/* данного узла, то при вызове этой функции переменная myData->role может
/* содержать значение UnknownRole. Поэтому, перед принятием
*/

```

```

/* решений на основе роли узла рекомендуется проверить, определено */
/* ли соответствующее значение. */
/* */
/*****/
static void unexpectedExceptionHandler(_INTRPT_Hndlr_Parms_T *exData) {
/*-----*/
/*
/* Создается указатель на структуру, в которой содержатся данные,
/* переданные программе обработки исключительных ситуаций.
/* */
/*-----*/
HandlerDataT *myData = (HandlerDataT *)exData->Com_Area;

/*-----*/
/*
/* Выполните необходимые действия по очистке. Обработчику отмены может
/* ситуаций может потребоваться глобальная информация, описывающая
/* этапы, выполненные перед сбоем. На их основе подбираются действия по
/* очистке. Эту информацию можно сохранить в структуре
/* HandlerDataT или в другом месте, доступном для этой функции.
/* */
/* */
/*-----*/

/*-----*/
/*
/* Если приложение запущено на основном узле, оно завершается.
/* Это необходимо потому, что программа выхода будет вызвана снова
/* с кодом действия Перезапустить, при этом функция restartCrg() всегда
/* должна работать однотипно. Кроме того, при завершении работы приложения*/
/* может стать ясно, что стало причиной исключительной ситуации.
/* По возможности предупредите пользователей и попросите их закрыть
/* приложение, чтобы можно было правильно обработать исключительную ситуацию.
/* */
/*-----*/

/*-----*/
endApplication(myData->actionCode,
myData->role,
myData->priorRole,
myData->crgData,
myData->epData);

/*-----*/
/*
/* Задается код возврата программы выхода.
/* */
/*-----*/
myData->retCode = QcstFailWithRestart;

/*-----*/
/*
/* Исключительной ситуации разрешается фильтрация стека вызовов.
/* */
/*-----*/
return;
} /* конец функции unexpectedExceptionHandler() */

/*****/

```

```

/* */
/* Эта функция вызывается при отмене задания, управляющего программой */
/* выхода. Задание может быть отменено по следующим причинам */
/* (список может быть неполным)- */
/* - Отмена активного CRG приложения с помощью API. API */
/* Завершить CRG, Выполнить принудительный перенос ресурсов, */
/* Остановить узел кластера, Удалить узел кластера и Удалить */
/* кластер отменяют задание, переданное на выполнение в момент, */
/* когда программа выхода уже была вызвана с кодом действия */
/* Запустить. */
/* - Отмена задания оператором с помощью одного из меню */
/* операционной системы. Например, Работа с активными заданиями. */
/* - Завершение работы подсистемы, в которой выполнялось это задание */
/* - Завершение работы всех подсистем */
/* - Выключение системы */
/* - Машинный сбой операционной системы */
/* */
/* Если отмена задания произошла до определения роли данного */
/* узла, то при вызове этой функции переменная myData->role может */
/* содержать значение UnknownRole. Поэтому, перед принятием решений на */
/* основе роли узла рекомендуется проверять, определено соответствующее */
/* значение. */
/* */
/*****/
static void cancelHandler(_CNL_Hndlr_Parms_T *cnlData) {

/*-----*/
/* */
/* Создается указатель на структуру, в которой содержатся данные, */
/* переданные программе обработки исключительных ситуаций. */
/* */

/*-----*/
HandlerDataT *myData = (HandlerDataT *)cnlData->Com_Area;

/*-----*/
/* */
/* Выполните необходимые действия по очистке. Обработчику отмены может */
/* потребоваться глобальная информация, описывающая этапы, выполненные */
/* перед отменой задания. На ее основе обработчик выясняет, полностью */
/* или частично завершилась функция, и определяет необходимость очистки. */
/* Эту информацию можно сохранить в структуре HandlerDataT */
/* или в любом другом месте, доступном для */
/* этой функции. */
/* */

/*-----*/

/*-----*/
/* */
/* Задание отменяется. Если приложение запущено с помощью кода */
/* действия Запустить или Перезапустить, то его работа завершается. */
/* Задание завершается вследствие изменения основного узла в результате */
/* применения API Принудительный перенос ресурсов, либо вследствие отмены */
/* задания пользователем с помощью команды CL, системного меню и т.п. */
/* */

/*-----*/
endApplication(myData->actionCode,
              myData->role,
              myData->priorRole,
              myData->crgData,

```

*/


```

        myData->epData);

/*-----*/
/*
/* Задается код возврата программы выхода.
/*
/*-----*/
    *myData->retCode = QcstSuccessful;

/*-----*/
/*
/* Возврат к операционной системе для окончательного завершения
/* задания.
/*
/*-----*/
    return;
} /* конец функции cancelHandler()

/*****
/*
/* Общая процедура, применяемая для завершения приложения с помощью
/* различных функций кода действия, программы обработки исключений и
/* программы обработки отмены заданий.
/*
/*****
static void endApplication(unsigned int actionCode,
                          int role,
                          int priorRole,
                          Qcst_EXTP0100_t *crgData,
                          EpData *epData) {

    if ( role == QcstPrimaryNodeRole
        &&
        crgData->Original_Cluster_Res_Grp_Stat == QcstCrgActive) {
/*-----*/
/*
/* Укажите здесь процедуры для завершения приложения. Кроме того,
/* вам может потребоваться указать процедуры, позволяющие
/* определить, если приложение все еще выполняется, так как эту
/* функцию можно вызвать только один раз для кода действия и второй
/* раз с помощью программы обработки отмены заданий (Например,
/* Завершить CRG).
/*
/*-----*/

/*-----*/
/*
/* После завершения приложения обновите область данных для отображения
/* того, что приложение больше не выполняется.
/*
/*-----*/
    setApp1CrgDataArea(App1_Ended);
}

    return;
} /* конец функции endApplication()

```

```

/*****
/*
/* Печать данных, переданных этой программе.
/*
/*
/*****
static void printParms(int actionCode,
                      int role,
                      int priorRole,
                      Qcst_EXTP0100_t *crgData,
                      EpData *epData) {

    unsigned int i;
    char *str;

    /* Печать кода действия
    printf("%s", "Action_Code = ");
    printActionCode(actionCode);

    /* Печать зависимых данных кода действия
    printf("%s", " Action_Code_Dependent_Data = ");
    switch (crgData->Action_Code_Dependent_Data) {
        case QcstNoDependentData: str = "QcstNoDependentData";
            break;
        case QcstMerge: str = "QcstMerge";
            break;
        case QcstJoin: str = "QcstJoin";
            break;
        case QcstPartitionFailure: str = "QcstPartitionFailure";
            break;
        case QcstNodeFailure: str = "QcstNodeFailure";
            break;
        case QcstMemberFailure: str = "QcstMemberFailure";
            break;
        case QcstEndNode: str = "QcstEndNode";
            break;
        case QcstRemoveNode: str = "QcstRemoveNode";
            break;
        case QcstApplFailure: str = "QcstApplFailure";
            break;
        case QcstResourceEnd: str = "QcstResourceEnd";
            break;
        case QcstDltCluster: str = "QcstDltCluster";
            break;
        case QcstRmvRcvyDmnNode: str = "QcstRmvRcvyDmnNode";
            break;
        case QcstDltCrg: str = "QcstDltCrg";
            break;
        default: str = "неизвестные зависимые данные кода действия";
    }
    printf("%s \n", str);

    /* Печать предыдущего кода действия
    printf("%s", " Prior_Action_Code = ");
    if (crgData->Prior_Action_Code)
        printActionCode(crgData->Prior_Action_Code);
    printf("\n");

    /* Печать имени кластера
    printStr(" Cluster_Name = ",
            crgData->Cluster_Name, sizeof(Qcst_Cluster_Name_t));

    /* Печать имени CRG.
    printStr(" Cluster_Resource_Group_Name = ",
            crgData->Cluster_Resource_Group_Name, sizeof(Qcst_Crg_Name_t));
    /* Печать типа CRG.
    printf("%s \n", " Cluster_Resource_Group_Type = QcstCrgApplResiliency");

```

```

/* Печать состояния CRG */
printf("%s", " Cluster_Resource_Group_Status = ");
printCrgStatus(crgData->Cluster_Resource_Group_Status);

/* Печать исходного состояния CRG */
printf("%s", " Original_Cluster_Res_Grp_Stat = ");
printCrgStatus(crgData->Original_Cluster_Res_Grp_Stat);

/* Печать имени очереди распределения информации */
printStr(" DI_Queue_Name = ",
crgData->DI_Queue_Name, sizeof(crgData->DI_Queue_Name));
printStr(" DI_Queue_Library_Name = ",
crgData->DI_Queue_Library_Name,
sizeof(crgData->DI_Queue_Library_Name));

/* Печать атрибутов CRG. */
printf("%s", " Cluster_Resource_Group_Attr = ");
if (crgData->Cluster_Resource_Group_Attr & QcstTcpConfigByUsr)
printf("%s", "Принятый IP-адрес настраивается пользователем");
printf("\n");

/* Печать ИД этого узла. */
printStr(" This_Nodes_ID = ",
crgData->This_Nodes_ID, sizeof(Qcst_Node_Id_t));

/* Печать роли этого узла. */
printf("%s %d \n", " роль этого узла = ", role);

/* Печать предыдущей роли этого узла. */
printf("%s %d \n", " предыдущая роль этого узла = ", priorRole);

/* Печать домена восстановления, из которого получен эта роль. */
printf("%s", " Node_Role_Type = ");
if (crgData->Node_Role_Type == QcstCurrentRcvyDmn)
printf("%s \n", "QcstCurrentRcvyDmn");
else
printf("%s \n", "QcstPreferredRcvyDmn");

/* Печать ИД изменяемого узла (если он существует). */
printStr(" Changing_Node_ID = ",
crgData->Changing_Node_ID, sizeof(Qcst_Node_Id_t));

/* Печать роли изменяемого узла (если он существует). */
printf("%s", " Changing_Node_Role = ");
if (crgData->Changing_Node_Role == -3)
printf("%s \n", "*LIST");
else if (crgData->Changing_Node_Role == -2)
printf("%s \n", "не применяется");
else
printf("%d \n", crgData->Changing_Node_Role);

/* Печать устойчивого IP-адреса. */
printStr(" Takeover_IP_Address = ",
crgData->Takeover_IP_Address, sizeof(Qcst_TakeOver_IP_Address_t));
/* Печать имени задания. */
printStr(" Job_Name = ", crgData->Job_Name, 10);

/* Печать изменений CRG. */
printf("%s \n", " Cluster_Resource_Group_Changes = ");
if (crgData->Cluster_Resource_Group_Changes & QcstRcvyDomainChange)
printf(" %s \n", "Изменен домен восстановления");
if (crgData->Cluster_Resource_Group_Changes & QcstTakeOverIpAddrChange)
printf(" %s \n", "Изменен принятый IP-адрес");

/* Печать времени ожидания восстановления после сбоя. */
printf("%s", "Failover_Wait_Time = ");
if (crgData->Failover_Wait_Time == QcstFailoverWaitForever)

```

```

    printf("%d %s \n", crgData->Failover_Wait_Time, "Время ожидания не ограничено");
else if (crgData->Failover_Wait_Time == QcstFailoverNoWait)
    printf("%d %s \n", crgData->Failover_Wait_Time, "Нулевое время ожидания");
else
    printf("%d %s \n", crgData->Failover_Wait_Time, "минут");

    /* Печать действия по умолчанию для восстановления после сбоя. */
printf("%s", "Failover_Default_Action = ");
    if (crgData->Failover_Default_Action == QcstFailoverProceed)
        printf("%d %s \n", crgData->Failover_Default_Action, "Продолжить");
else
    printf("%d %s \n", crgData->Failover_Default_Action, "Отмена");
/* Печать имени очереди сообщений восстановления после сбоя. */
printStr(" Failover_Msg_Queue = ",
        crgData->Failover_Msg_Queue, sizeof(crgData->Failover_Msg_Queue));
printStr(" Failover_Msg_Queue_Lib = ",
        crgData->Failover_Msg_Queue_Lib,
        sizeof(crgData->Failover_Msg_Queue_Lib));

    /* Печать версии кластера. */
printf("%s %d \n",
        " Cluster_Version = ", crgData->Cluster_Version);

    /* Печать уровня модификации версии кластера. */
printf("%s %d \n",
        " Cluster_Version_Mod_Level = ",
        crgData->Cluster_Version_Mod_Level);

    /* Печать запрашивающего пользовательского профайла. */
printStr(" Req_User_Profile = ",
        crgData->Req_User_Profile, sizeof(crgData->Req_User_Profile));
/* Печать длины данных структуры. */
printf("%s %d \n",
        " Length_Info_Returned = ", crgData->Length_Info_Returned);
/* Печать смещения массива домена восстановления. */
printf("%s %d \n",
        " Offset_Rcvy_Domain_Array = ", crgData->Offset_Rcvy_Domain_Array);
/* Печать числа узлов массива домена восстановления. */
printf("%s %d \n",
        " Number_Nodes_Rcvy_Domain = ",
        crgData->Number_Nodes_Rcvy_Domain);

    /* Печать текущего/нового домена восстановления. */
printRcvyDomain(" Домен восстановления:",
        crgData->Number_Nodes_Rcvy_Domain,
        (Qcst_Rcvy_Domain_Array1_t *)
        ((char *)crgData + crgData->Offset_Rcvy_Domain_Array));
/* Печать смещения массива предыдущего домена восстановления. */
printf("%s %d \n",
        " Offset_Prior_Rcvy_Domain_Array = ",
        crgData->Offset_Prior_Rcvy_Domain_Array);

    /* Печать числа узлов массива предыдущего домена восстановления. */
printf("%s %d \n",
        " Number_Nodes_Prior_Rcvy_Domain = ",
        crgData->Number_Nodes_Prior_Rcvy_Domain);

    /* Печать предыдущего домена восстановления, если он был передан. */
if (crgData->Offset_Prior_Rcvy_Domain_Array) {
    printRcvyDomain(" Предыдущий домен восстановления:",
        crgData->Number_Nodes_Prior_Rcvy_Domain,
        (Qcst_Rcvy_Domain_Array1_t *)
        ((char *)crgData + crgData->Offset_Prior_Rcvy_Domain_Array));
}

return;
} /* конец функции printParms() */

```

```

/*****/
/*
/* Печать строки кода действия.
/*
/*****/
static void printActionCode(unsigned int ac) {

    char *code;
    switch (ac) {
        case QcstCrgAcInitialize: code = "QcstCrgAcInitialize";
                                break;
        case QcstCrgAcStart:      code = "QcstCrgAcStart";
                                break;
        case QcstCrgAcRestart:   code = "QcstCrgAcRestart";
                                break;
        case QcstCrgAcEnd:       code = "QcstCrgAcEnd";
                                break;
        case QcstCrgAcDelete:    code = "QcstCrgAcDelete";
                                break;
        case QcstCrgAcReJoin:    code = "QcstCrgAcReJoin";
                                break;
        case QcstCrgAcFailover:  code = "QcstCrgAcFailover";
                                break;
        case QcstCrgAcSwitchover: code = "QcstCrgAcSwitchover";
                                break;
        case QcstCrgAcAddNode:   code = "QcstCrgAcAddNode";
                                break;
        case QcstCrgAcRemoveNode: code = "QcstCrgAcRemoveNode";
                                break;
        case QcstCrgAcChange:    code = "QcstCrgAcChange";
                                break;
        case QcstCrgAcDeleteCommand: code = "QcstCrgAcDeleteCommand";
                                break;
        case QcstCrgAcUndo:      code = "QcstCrgAcUndo";
                                break;
        case QcstCrgAcEndNode:   code = "QcstCrgAcEndNode";
                                break;
        case QcstCrgAcAddDevEnt: code = "QcstCrgAcAddDevEnt";
                                break;
        case QcstCrgAcRmvDevEnt: code = "QcstCrgAcRmvDevEnt";
                                break;
        case QcstCrgAcChgDevEnt: code = "QcstCrgAcChgDevEnt";
                                break;
        case QcstCrgAcChgNodeStatus: code = "QcstCrgAcChgNodeStatus";
                                break;
        case QcstCrgAcCancelFailover: code = "QcstCrgAcCancelFailover";
                                break;
        case QcstCrgAcVerificationPhase: code = "QcstCrgAcVerificationPhase";
                                break;
        default:                  code = "unknown action code";
                                break;
    }
    printf("%s", code);

    return;
} /* конец функции printActionCode() */

/*****/
/*
/* Печать состояния CRG
/*
/*****/
static void printCrgStatus(int status) {

    char * str;

```

```

switch (status) {
    case QcstCrgActive:          str = "QcstCrgActive";
                                break;
    case QcstCrgInactive:       str= "QcstCrgInactive";
                                break;
    case QcstCrgIndoubt:        str = "QcstCrgIndoubt";
                                break;
    case QcstCrgRestored:       str = "QcstCrgRestored";
                                break;
    case QcstCrgAddnodePending: str = "QcstCrgAddnodePending";
break;
    case QcstCrgDeletePending:  str = "QcstCrgDeletePending";
                                break;
    case QcstCrgChangePending:  str = "QcstCrgChangePending";
                                break;
    case QcstCrgEndCrgPending:  str = "QcstCrgEndCrgPending";
                                break;
    case QcstCrgInitializePending: str = "QcstCrgInitializePending";
break;
    case QcstCrgRemovenodePending: str = "QcstCrgRemovenodePending";
break;
    case QcstCrgStartCrgPending: str = "QcstCrgStartCrgPending";
break;
    case QcstCrgSwitchOverPending: str = "QcstCrgSwitchOverPending";
break;
    case QcstCrgDeleteCmdPending: str = "QcstCrgDeleteCmdPending";
break;
    case QcstCrgAddDevEntPending: str = "QcstCrgAddDevEntPending";
break;
    case QcstCrgRmvDevEntPending: str = "QcstCrgRmvDevEntPending";
break;
    case QcstCrgChgDevEntPending: str = "QcstCrgChgDevEntPending";
break;
    case QcstCrgChgNodeStatusPending: str = "QcstCrgChgNodeStatusPending";
break;
    default: str = "неизвестное состояние CRG";
}
printf("%s \n", str);

return;
} /* конец функции printCrgStatus() */

/*****
/*
/* Печать домена восстановления.
/*
/*
*****/
static void printRcvyDomain(char *str,
                           unsigned int count,
                           Qcst_Rcvy_Domain_Array1_t *rd) {

    unsigned int i;
    printf("\n %s \n", str);
    for (i=1; i<=count; i++) {
        printStr("    Node_ID = ", rd->Node_ID, sizeof(Qcst_Node_Id_t));
    printf("%s %d \n", "    Node_Role = ", rd->Node_Role);
        printf("%s", "    Membership_Status = ");
        switch (rd->Membership_Status) {
            case 0: str = "Активен";
                    break;
            case 1: str = "Неактивен";
                    break;
            case 2: str = "Раздел";
                    break;
            default: str = "неизвестное состояние узла";
        }
    }
}

```

```

    printf("%s \n", str);
    rd++;
}
return;
} /* конец функции printRcvyDomain() */
/*****
/*
/* Объединяет строку, оканчивающуюся символом NULL со строкой, не
/* оканчивающейся символом NULL, и распечатывает результат.
/*
/*
/*****
static void printStr(char *s1, char *s2, unsigned int len) {

    char buffer[132];
    memset(buffer, 0x00, sizeof(buffer));
    memcpy(buffer, s1, strlen(s1));
    strcat(buffer, s2, len);
    printf("%s \n", buffer);
    return;
} /* конец функции printStr */

```

Планирование устойчивости данных

Устойчивость данных означает, что данные всегда доступны пользователям и приложениям. Устойчивость данных обеспечивается применением технологий кластеров i5/OS с переносимыми дисками, распределенным зеркальным копированием или логической репликацией.

В i5/OS поддерживаются различные технологии для обеспечения устойчивости данных. Вместе с функциями кластеров i5/OS эти технологии позволяют создать полное решение высокой готовности. Эти технологии можно классифицировать следующим образом:

Независимый пул дисков i5/OS

Эти технологии основаны на реализации независимых пулов дисков в i5/OS. Решение высокой готовности, которое использует независимый пул дисков, сохраняет устойчивые данные в независимом пуле дисков. Во многих случаях для этого требуется перенос данных в независимый пул дисков. Далее предполагается, что этот перенос уже выполнен.

На основе независимых пулов дисков работают следующие функции i5/OS:

- Переносимые диски
- Географическая зеркальная защита
- Синхронное зеркальное копирование
- Глобальное зеркальное копирование

Логическая репликация

Логическая репликация - это технология, основанная на ведении журнала, и позволяющая осуществлять репликацию данных в реальном времени. Технологии логической репликации применяют службы ресурсов кластера i5/OS и ведение журнала с помощью приложений деловых партнеров IBM. Эти решения предполагают, что среду высокой готовности настраивает приложение делового партнера. Здесь не описаны никакие особые требования для этих решений деловых партнеров IBM. При развертывании логической репликации в решении высокой готовности обратитесь к справке приложения или к специалисту по обслуживанию.

Информация, связанная с данной



IBM eServer iSeries Independent ASPs: A Guide to Moving Applications to IASPs

Выбор данных, которые должны быть устойчивыми

Определите, какие данные должны быть устойчивыми.

Эта процедура схожа с отбором данных для резервного копирования. Вам нужно определить, какие данные наиболее важны для вашего предприятия.

Например, если ваша организация занимается бизнесом в Internet, то наибольшую важность могут представлять следующие данные:

- Заказы, полученные сегодня
- Склад
- Информация о клиентах

Вряд ли стоит обеспечивать устойчивость данных, которые изменяются крайне редко и не участвуют в повседневной работе.

Планирование переключаемых дисков

Хранится только одна копия данных, которая размещена на переносимом аппаратном обеспечении - либо во внешнем блоке, либо в IOP логического раздела.

В случае сбоя главного узла точка доступа к ресурсу переносится на один из резервных узлов. Кроме того, независимые ASP можно применять в среде зеркальной защиты, распределенной по сайтам (XSM). Такой подход позволяет для обеспечения лучшей готовности и защиты создать и поддерживать зеркальную копию независимого ASP в системе, расположенной в удаленном офисе.

Применение распределенной по сайтам зеркальной защиты (XSM) или независимых ASP в качестве переносимых ресурсов кластера требует тщательного планирования.

Также следует оценить текущую конфигурацию дисков системы для определения потребности в дополнительных дисковых накопителях. Как и в любой конфигурации дисков системы, число накопителей, доступных для приложения, может в значительной степени влиять на его быстродействие. Дополнительная нагрузка на ограниченное число дисковых накопителей может приводить к увеличению времени ожидания дисков и значительному росту времени ответов на запросы приложения. Это особенно важно в отношении временной памяти в системе, настроенной с независимыми пулами дисков. Вся временная память записывается в дисковый пул SYSBAS. Если приложением используется только небольшой объем временной памяти, можно работать с меньшим числом дисков в пуле SYSBAS. Также необходимо учитывать, что дисковый пул SYSBAS используется операционной системой и базовыми функциями.

Перед тем как использовать IBM Systems Director Navigator for i5/OS для выполнения задач управления дисками, например, для создания независимого пула дисков, необходимо настроить соответствующие права доступа для специальных сервисных средств (DST).

Задачи, связанные с данной

Включение дисковых накопителей и обращение к ним

Требования к аппаратному обеспечению для переносимых дисков:

Для использования переносимых дисков требуется специальное аппаратное обеспечение.

Для использования переносимых дисков необходим один из следующих компонентов:

- Один или несколько блоков расширения (стоек/блоков), расположенные в цепи высокоскоростного канала (HSL).
- Один или несколько IOP на общей шине или IOP, назначенный для пула ввода-вывода. В среде LPAR можно переносить IOP, содержащий независимые переносимые диски, из одного раздела системы в другой без блока расширения. IOP должен располагаться на шине, совместно используемой множественными разделами или назначенной для пула ввода-вывода. Будут перенесены все адаптеры ввода-вывода на IOP.

Кроме этих требований к аппаратному обеспечению, для переносимых дисков необходимо планирование физической конфигурации:

- Для соединения блоков расширения с системами в кластере необходимо использовать кабели высокоскоростных каналов (HSL). В цепи HSL блок расширения должен физически располагаться рядом с другой системой или блоком расширения, владельцем которого является другая система. В цепь каждого HSL можно включить не более двух систем (узлов кластера), в то время как каждая система может быть подключена ко многим цепям HSL. Цепь каждого HSL может включать не более четырех блоков расширения, а отдельный сегмент цепи должен содержать не более трех блоков расширения. В цепи HSL с двумя системами находятся два сегмента, разделенные этими системами. Все блоки расширения отдельного сегмента цепи должны содержаться в одной и той же группе ресурсов кластера устройства (CRG).
- Блок расширения становится переносимым, если он физически расположен дальше остальных от системы в пределах сегмента цепи. Примечание: при попытке сделать переносимым блок расширения, предшествующий другому блоку расширения, который расположен еще дальше от системы владельца и не является переносимым, произойдет ошибка.
- Переносимый блок расширения должен быть соединен в сети управления питанием системы с системным блоком, который будет изначально назначен основным узлом группы ресурсов кластера устройств (CRG устройств). Главным узлом может быть основной или дополнительный логический раздел системного блока. Владелец этого блока расширения при использовании логических разделов должен быть раздел, который участвует в кластере.

Требования переносимых дисков к программному обеспечению:

Если планируется использовать переносимые диски для обеспечения высокой готовности i5/OS, убедитесь, что выполнены минимальные требования к программному обеспечению.

- Для использования новых и усовершенствованных функций и возможностей этой технологии рекомендуется установить последний выпуск и версию операционной системы в каждой системе или логическом разделе, которые участвуют в решении высокой готовности, основанном на этой технологии.

Примечание: Для систем в одном высокоскоростном кольце HSL просмотрите информацию на Web-сайте по высокой готовности, чтобы убедиться в совместимости версий i5/OS.

- Для выполнения некоторых задач управления дисками для реализации независимых пулов дисков требуется один из следующих графических интерфейсов.
 - IBM Systems Director Navigator для i5/OS
 - System i Navigator
- Необходимо установить компонент 41 i5/OS HA Switchable Resources. Компонент 41 дает возможность переносить независимые пулы дисков между системами. Для переноса независимого пула дисков между системами эти системы должны входить в кластер, а независимый пул дисков должен быть связан с группой ресурсов кластера устройств в этом кластере. Компонент 41 также необходим для работы с интерфейсами управления высокой готовности, которые являются частью лицензионной программы IBM System i High Availability Solutions Manager (iHASM).

Информация, связанная с данной

Высокая готовность и кластеры

Требования к средствам связи для коммутируемого диска:

Коммутируемым дискам требуется по меньшей мере один интерфейс связи TCP/IP для связи между системами в кластере.

В целях резервирования рекомендуется иметь по меньшей мере два отдельных интерфейса для связи между системами.

Планирование распределенной по сайтам зеркальной защиты

Распределенная по сайтам зеркальная защита обеспечивает несколько методик восстановления после аварии и обеспечения высокой готовности i5/OS: географическая зеркальная защита, синхронное зеркальное копирование и глобальное зеркальное копирование.

Методики распределенной по сайтам зеркальной защиты реализуют восстановление после аварии посредством обслуживания отдельных узлов, которые обычно находятся на некотором расстоянии друг от друга. Каждая из методик выдвигает определенные требования к соединениям, аппаратному и программному обеспечению. Однако перед внедрением одной из этих методик следует выполнить планирование узлов. Один из узлов обычно считается рабочим, или исходным узлом. Он содержит рабочие данные, которые копируются на удаленный узел. Удаленный узел, который иногда называется резервным или целевым узлом, содержит зеркальную копию рабочих данных. В случае аварии рабочего узла резервный узел поддерживает работу предприятия, используя зеркальную копию данных. Перед настройкой технологии распределенной по сайтам зеркальной защиты следует учесть следующие вопросы при планировании узлов.

Определите рабочие и резервные узлы

Просмотрите аппаратные и программные ресурсы на каждом из узлов, чтобы определить, все ли необходимые для решения распределенной по сайтам зеркальной защиты компоненты имеются.

Определите расстояние между рабочим и резервным узлами

В зависимости от пропускной способности соединения и других факторов расстояние между узлами может влиять на производительность и латентность выбранной технологии зеркального копирования. Некоторым технологиям распределенной по сайтам зеркальной защиты лучше подходят для узлов, находящихся на больших расстояниях друг от друга, а при использовании других может наблюдаться снижение производительности.

Убедитесь, что у вас имеются необходимые права доступа к DST

Перед тем как использовать IBM Systems Director Navigator for i5/OS для выполнения задач управления дисками, необходимо настроить соответствующие права доступа для специальных сервисных средств (DST).

Задачи, связанные с данной

Включение дисковых накопителей и обращение к ним

Планирование географической зеркальной защиты:

Географическая зеркальная защита является дополнительной функцией распределенной по сайтам зеркальной защиты. Эта технология обеспечивает восстановление после аварии и высокую готовность в средах i5/OS.

Требования к аппаратному обеспечению для географической зеркальной защиты:

Если требуется использовать географическую зеркальную защиту для высокой готовности i5/OS, убедитесь, что соблюдены минимальные требования к аппаратному обеспечению.

- Должны быть удовлетворены требования независимого пула дисков к аппаратному обеспечению.
- Необходимы по крайней мере две модели System i, которые могут быть разделены географически.
- Необходимо, чтобы в каждом расположении находилось по крайней мере два набора дисков одинаковой емкости.
- Требуется настроить отдельный пул памяти для заданий с использованием независимых пулов дисков с географической зеркальной защитой. При реализации географической зеркальной защиты с использованием пула оперативной памяти может произойти зависание системы по причине перегрузки.
- Географическая зеркальная защита реализуется при доступном пуле дисков. При реализации географической зеркальной защиты не разрешено изменять системное значение времени дня (QTIME).
- Также важно соблюдать требования к средствам связи для независимых пулов дисков, поскольку они влияют на производительность.

Понятия, связанные с данным

“Требования к средствам связи для географической зеркальной защиты” на стр. 51

При реализации решения высокой готовности i5/OS, которое использует географическую зеркальную защиту, необходимо составить такой план линий связи, чтобы поток данных зеркальной защиты не оказывал побочное влияние на производительность системы.

Требования к программному обеспечению для географической зеркальной защиты:

Если требуется использовать географическую зеркальную защиту как часть решения высокой производительности i5/OS, необходимо следующее программное обеспечение.

- Для использования дополнительных функций географической зеркальной защиты требуется IBM System i High Availability Solutions Manager (iHASM) номер лицензионной программы (5761-HAS).
- Для использования новых и усовершенствованных функций и возможностей этой технологии рекомендуется установить последний выпуск и версию операционной системы в каждой системе или логическом разделе, которые участвуют в решении высокой готовности, основанном на этой технологии.

Примечание: Для систем в в одном высокоскоростном кольце HSL просмотрите информацию на Web-сайте по высокой готовности, чтобы убедиться в совместимости версий i5/OS.

- Для выполнения некоторых задач управления дисками для реализации независимых пулов дисков требуется один из следующих графических интерфейсов.
 - IBM Systems Director Navigator для i5/OS
 - System i Navigator
- Необходимо установить компонент 41 i5/OS HA Switchable Resources. Компонент 41 дает возможность переносить независимые пулы дисков между системами. Для переноса независимого пула дисков между системами эти системы должны входить в кластер, а независимый пул дисков должен быть связан с группой ресурсов кластера устройств в этом кластере. Компонент 41 также необходим для работы с интерфейсами управления высокой готовности, которые являются частью лицензионной программы IBM System i High Availability Solutions Manager (iHASM).

Информация, связанная с данной

Высокая готовность и кластеры

Требования к средствам связи для географической зеркальной защиты:

При реализации решения высокой готовности i5/OS, которое использует географическую зеркальную защиту, необходимо составить такой план линий связи, чтобы поток данных зеркальной защиты не оказывал побочное влияние на производительность системы.

Воспользуйтесь следующими рекомендациями:

- Географическая зеркальная защита может создать объемный поток данных. Если географическая зеркальная защита использует соединение IP совместно с другим приложением, например кластерным, то она может блокироваться, что приведет к синхронизации. Кроме того, ответ кластера может оказаться недоступным, что станет причиной появления отделившихся узлов. Географической зеркальной защите требуются собственные линии связи. Без собственной линии связи она может конкурировать за ресурсы системы с другими приложениями, использующими ту же линию связи, и снижать быстродействие и производительность пользовательской сети. Кроме того, возможность негативного влияния на контроль пульса кластера приводит к распаду кластера. Поэтому отдельные линии связи требуются как для географической зеркальной защиты, так и для кластеров. Географическая зеркальная защита поддерживает до четырех линий связи.

Для оптимизации производительности географическая зеркальная защита отправляет изменения по нескольким линиям. Данные передаются по каждой линии связи от первой до четвертой по очереди, и цикл возобновляется. Четыре линии связи обеспечивают наибольшее быстродействие, но можно достичь относительно высокой производительности и с двумя линиями.

Если для географической зеркальной защиты вы используете несколько линий связи между узлами, то размещение этих линий в разных подсетях позволит сбалансировать их использование в обеих системах.

- Если конфигурация требует использования одной и той же линии связи несколькими приложениями или службами, то некоторые подобные ситуации можно исправить с помощью реализации Quality of Service (QoS) с использованием функций TCP/IP i5/OS. Стратегии QoS i5/OS позволяют зарезервировать приоритет и пропускную способность сети для приложений TCP/IP.

- | Если для географической зеркальной защиты вы используете несколько линий связи между узлами, то размещение этих линий в разных подсетях позволит сбалансировать их использование в обеих системах.
- | • Убедитесь, что производительность всех соединений портов данных одинакова. Это означает, что все соединения между парами систем должны иметь одинаковую скорость и тип соединения. При различной производительности быстродействие установится на уровне самого медленного соединения.
- | • Настройка виртуальной частной сети для соединений TCP/IP дает следующие преимущества:
 - | – Безопасность передачи данных благодаря их шифрованию
 - | – Повышенная надежность передачи данных благодаря большому объему резервирования

Понятия, связанные с данным

| “Требования к аппаратному обеспечению для географической зеркальной защиты” на стр. 50
| Если требуется использовать географическую зеркальную защиту для высокой готовности i5/OS, убедитесь, что соблюдены минимальные требования к аппаратному обеспечению.

Ссылки, связанные с данной

| Quality of Service (QoS)

Планирование ведения журнала для географической зеркальной защиты:

При реализации высокой готовности на основе географической зеркальной защиты i5/OS необходимо составить план ведения журнала.

Журнал позволяет сохранить информацию о транзакциях в случае его аварийного выключения. Система заносит в журнал информацию обо всех изменениях объекта. Независимо от реализуемого решения высокой готовности ведение журнала является наилучшим способом предотвращения потери данных при аварийных простоях системы.

Информация, связанная с данной

Управление журналами

Планирование резервного копирования для географической зеркальной защиты:

| Для реализации высокой готовности на основе географической зеркальной защиты необходимо получить представление о стратегии создания резервных копий в этом окружении и запланировать ее внедрение.

| Если требуется изменить стратегию резервного копирования, то это необходимо сделать до настройки любого решения высокой готовности. Географическая зеркальная защита не поддерживает одновременный доступ к зеркальной копии независимого пула дисков, который может участвовать в удаленном резервном копировании. Для резервного копирования зеркальной копии на магнитную ленту приостановите зеркальную защиту рабочей системы и отсоедините зеркальную копию со включенным мониторингом. Мониторинг позволяет следить за изменениями в рабочей копии таким образом, чтобы они синхронизировались при возвращении зеркальной копии в активное состояние. После этого необходимо включить отсоединенную копию независимого пула дисков, создать резервную копию, выключить независимый пул дисков и вновь соединить его с исходной рабочей системой. Для этого процесса требуется только частичная синхронизация данных рабочей и зеркальной копии.

| Во время резервного копирования и синхронизации система остается незащищенной. Также рекомендуется приостановить зеркальную защиту со включенным мониторингом, что ускорит синхронизацию. Кроме этого синхронизация требуется в случае каких-либо простоев постоянной передачи, например при потере всех соединений между исходной и целевой системой в течение длительного периода времени. Также во избежание рисков, связанных со сбоями соединения можно использовать избыточные средства связи.

| Рекомендуется также использовать географическую зеркальную защиту по крайней мере в трех системах или логических разделах, чтобы рабочая копия независимого пула дисков могла быть перенесена в другую систему в том же расположении, в котором поддерживается географическая зеркальная защита.

Понятия, связанные с данным

“Сценарий: Резервное копирование в среде с географической зеркальной защитой” на стр. 113
В сценарии дано общее представление о задачах, которые необходимо выполнить при удаленном резервном копировании решения высокой готовности i5/OS, которое использует географическую зеркальную защиту.

“Сценарий: Коммутируемый диск с географической зеркальной защитой” на стр. 78
В данном сценарии описано решение высокой готовности i5/OS, использующее коммутируемые диски с географической зеркальной защитой в кластере с тремя узлами. Данное решение обеспечивает как восстановление после аварии, так и высокую готовность.

Планирование производительности для географической зеркальной защиты:

При реализации решения с географической зеркальной защитой требуется располагать полной информацией для планирования среды с минимальным влиянием на производительность.

На производительность географической зеркальной защиты влияют различные факторы. Общие рекомендации по планированию для максимального увеличения производительности в среде с географической зеркальной защитой обусловлены следующими факторами:

Рекомендации относительно CPU

Географическая зеркальная защита увеличивает загрузку CPU, поэтому ему требуется достаточная избыточная производительность. Для увеличения производительности CPU вам могут понадобиться дополнительные процессоры. Как правило, для разделов с использованием географической зеркальной защиты требуется больше, чем просто отдельный процессор. При минимальной конфигурации CPU дополнительная нагрузка на CPU при использовании географической зеркальной защиты может составить 5 - 20%. Если в зеркальной системе меньше процессоров, чем в рабочей, то при большом количестве операций записи дополнительная нагрузка на CPU может оказаться значительной и повлиять на производительность.

Рекомендации относительно объема машинного пула

Для наилучшей производительности географической зеркальной защиты, например, при синхронизации, увеличьте объем машинного пула по крайней мере на такое значение, которое вычисляется по следующей формуле:

- Объем дополнительного хранилища машинного пула: $300 \text{ Мб} + 0,3\text{Мб} \times \text{количество ARM дисков в независимом пуле дисков}$. В следующих примерах показан объем дополнительного хранилища машинного пула, требуемый для независимых пулов дисков с 90 ARM дисков и 180 ARM дисков соответственно:

- $300 + (.3 \times 90 \text{ ARM}) = 327 \text{ Мб}$ дополнительного хранилища машинного пула

- $300 + (.3 \times 180 \text{ ARM}) = 354 \text{ Мб}$ дополнительного хранилища машинного пула

Дополнительный объем хранилища машинного пула необходим на всех узлах группы ресурсов кластера (CRG) для обеспечения достаточного объема хранилища на узлах-получателях в случае принудительного или автоматического переноса ресурсов. Как обычно, чем большее число дисковых накопителей находится в независимом пуле дисков, тем выше становится производительность, поскольку большее количество операций можно смогут выполняться параллельно.

Для того чтобы функция настройки производительности не уменьшала размер машинного пула, выполните одно из следующих действий:

1. Установите для минимального объема машинного пула вычисленное значение (текущее значение плюс дополнительный объем для географической зеркальной защиты из формулы) с помощью команды Работа с общими пулами памяти (WRKSHRPOOL) или команды Изменить общий пул памяти (CHGSHRPOOL).

Примечание: Эту опцию рекомендуется использовать с опцией Работа с общими пулами памяти (WRKSHRPOOL).

- | 2. Установите системное значение опции Автоматически настраивать пулы памяти и уровни активности (QPFRADJ), чтобы запретить функции настройки производительности изменять размер машинного пула.

| **Рекомендации относительно дискового накопителя**

| Производительность дискового накопителя и IOA может влиять на общую производительность географической зеркальной защиты. Это становится особенно заметным, если дисковая подсистема в зеркальной системе более медленная. При работе географической зеркальной защиты в синхронном режиме все операции записи в рабочей копии ограничены операциями записи на диск, производимыми зеркальной копией. Поэтому в случае медленной целевой дисковой подсистеме быстродействие источника будет ограничено. Это влияние на производительность снижается при работе географической зеркальной защиты в асинхронном режиме. Работа в асинхронном режиме уменьшает влияние ожидания ответа дисковой подсистемы на целевой стороне и отправляет исходной стороне подтверждение, когда измененная страница памяти оказывается в памяти на целевой стороне.

| **Рекомендации относительно системного пула дисков**

| Как и при любой другой конфигурации диска, количество дисковых накопителей, доступных приложению, может значительно влиять на его производительность. Дополнительная нагрузка на ограниченное число дисковых накопителей может привести к более длительному ожиданию дисков и намного более продолжительному времени их ответа на запросы приложения. Это, в частности, важно, когда речь идет о временном хранилище в системе с независимыми пулами дисков. Все содержимое временного хранилища записывается в пул дисков SYSBAS. Если приложение не использует достаточного объема временного хранилища, то можно уменьшить число дисков в пуле дисков SYSBAS. Также необходимо помнить, что операционная система и базовые функции работают в пуле дисков SYSBAS.

| **Рекомендации относительно параметров сети**

| Сетевые соединения и параметры могут влиять на производительность географической зеркальной защиты. Необходимо не только убедиться, что сетевая адресация настроена для каждого набора IP-адресов порта данных в различных подсетях, но и одинаково настроить сетевые соединения и параметры.

Планирование синхронного зеркального копирования:

Решения высокой готовности i5/OS поддерживают синхронное зеркальное копирование, которое обеспечивает высокую готовность и восстановление после сбоев. Для применения этой технологии в решении высокой готовности необходимо соответствующее планирование.

Информация, связанная с данной



Рекомендации по работе с функциями служб копирования в DS6000



Рекомендации по работе с функциями служб копирования в DS8000

Требования к аппаратному обеспечению для синхронного зеркального копирования:

В этом разделе описаны требования к аппаратному обеспечению, которые должны быть удовлетворены для применения синхронного зеркального копирования в решении высокой готовности для i5/OS.

Далее описаны минимальные требования к аппаратному обеспечению:

- Необходимы как минимум две модели System i, расположенные в разных местах, к каждой из которых подключен хотя бы один внешний накопитель IBM System Storage DS6000 или DS8000. Внешние накопители DS6000 и DS8000 поддерживаются для всех моделей System i, к которым возможно подключение внешней памяти по технологии Fibre Channel.
- Необходима одна из перечисленных моделей адаптеров Fibre Channel:
 - Контроллер дисков 2766 2 Gigabit Fibre Channel PCI

- Контроллер дисков 2787 2 Gigabit Fibre Channel PCI-X
- Контроллер дисков 5760 4 Gigabit Fibre Channel PCI-X
- Для поддержки внешнего загрузочного накопителя для DS6000 or DS8000 требуется новый процессор ввода-вывода:
 - Компонент 2847 PCI-X IOP для SAN
- Перед началом настройки необходимо соответствующим образом подготовить диски. Один набор дисков потребуются для источника, такой же набор - для целевого объекта, и по одному набору дисков для каждой копии, обеспечивающей согласованность данных.

Информация, связанная с данной

 [iSeries™ и IBM TotalStorage: Руководство по применению внешнего диска в системе i5](#)

 [IBM System Storage DS6000 Information Center](#)

 [IBM System Storage DS8000 Information Center](#)

Требования к программному обеспечению для синхронного зеркального копирования:

В этом разделе описаны требования к программному обеспечению, которые должны быть удовлетворены для применения синхронного зеркального копирования в решении высокой готовности для i5/OS.

Для применения синхронного зеркального копирования необходимо выполнение следующих условий:

- Каждая модель System i в решении высокой готовности должна работать под управлением i5/OS V6R1, чтобы применялась лицензионная программа IBM System i High Availability Solutions Manager (iHASM) (5761-HAS).

Примечание: В предыдущих выпусках можно по-прежнему использовать Службы копирования IBM для System i, предлагаемые Lab Services, чтобы работать с решениями IBM System Storage. Если глобальное зеркальное копирование применяется на нескольких платформах, или если требуется реализовать глобальное зеркальное копирование на нескольких разделах System i, то также можно использовать Службы копирования IBM для System i.

- в каждой системе, участвующей в решении высокой готовности с применением синхронного зеркального копирования, должна быть установлена лицензионная программа IBM System i High Availability Solutions Manager (iHASM) (5761-HAS).
- Должен быть установлен компонент i5/OS 41 HA Switchable Resources. Компонент 41 предоставляет функции переключения независимых пулов дисков между системами. Для возможности переключения независимых пулов дисков между системами эти системы должны входить в кластер, а в кластере с группой ресурсов кластера должен быть связан независимый переключаемый диск. Компонент 41 также требуется для работы с интерфейсами управления высокой готовности, поставляемыми как часть лицензионной программы IBM System i High Availability Solutions Manager (iHASM).
- Лицензионная программа iHASM использует интерфейс командной строки памяти (DSCLI) для управления памятью. DSCLI является обязательным программным компонентом для всех решений IBM System Storage. DSCLI должен быть установлен во всех системах или разделах, участвующих в решении высокой готовности, в котором применяется любая из технологий IBM System Storage, такая как мгновенное копирование, синхронное зеркальное копирование или глобальное зеркальное копирование. Для применения DSCLI необходимо также наличие следующих компонентов:
 - Java версии 1.4
 - Компонент 35 (поставщик услуг шифрования CCA), установленный в системе или разделе
- Необходимо установить последние PTF.

Информация, связанная с данной

 [iSeries™ и IBM TotalStorage: Руководство по применению внешнего диска в системе i5](#)

 [IBM System Storage DS6000 Information Center](#)

 [IBM System Storage DS8000 Information Center](#)

Требования к связи для синхронного зеркального копирования:

В этом разделе описаны требования к связи, которые должны быть удовлетворены для применения синхронного зеркального копирования в решении высокой готовности для i5/OS.


Для того чтобы использовать технологию синхронного зеркального копирования, необходимо применять или запланировать применение сети хранения данных (SAN).

SAN - это специализированная централизованная инфраструктура защиты информации, которая обеспечивает многоканальную связь между точками системы и устройствами хранения данных. Технология SAN применяется для решений на основе IBM System Storage, таких как внешние накопители DS8000 или DS6000.

Далее описаны минимальные требования к связи для решения высокой готовности i5/OS, применяющего синхронное зеркальное копирование:

- Необходима одна из перечисленных моделей адаптеров Fibre Channel:
 - Контроллер дисков 2766 2 Gigabit Fibre Channel PCI
 - Контроллер дисков 2787 2 Gigabit Fibre Channel PCI-X
 - Контроллер дисков 5760 4 Gigabit Fibre Channel PCI-X
- Продукт System i поддерживает различные типы коммутаторов SAN. Полный список поддерживаемых коммутаторов приведен на Web-сайте Storage area network (SAN).
- Для повышения общей устойчивости и производительности рекомендуется воспользоваться функциями многоканального ввода-вывода. Многоканальный ввод-вывод позволяет применять несколько устройств Fibre Channel, подключенных к одним и тем же логическим дискам в накопителе. При правильной настройке это позволяет избежать сбоев при отказе отдельных устройств, блоков ввода-вывода или даже колец HSL. Многоканальный ввод-вывод также улучшает производительность за счет распределения нагрузки по доступным каналам. Каждое из альтернативных подключений дискового накопителя является независимым. Наличие нескольких подключений улучшает устойчивость данных, допуская работу с дисковой памятью даже в случае сбоя одного из каналов.

Ссылки, связанные с данной

 [Web-сайт Storage area network \(SAN\)](#)

Планирование журнала для синхронного зеркального копирования:

Журналы являются важной частью стратегии восстановления для всех решений высокой готовности. В таких технологиях IBM System Storage, как синхронное зеркальное копирование, ведение журнала применяется для принудительной записи в внешние устройства памяти, поскольку зеркальное копирование данных выполняется вне памяти System i.

Журнал позволяет сохранить информацию о транзакциях в случае его аварийного выключения. Система заносит в журнал информацию обо всех изменениях объекта. Независимо от реализуемого решения высокой готовности ведение журнала является наилучшим способом предотвращения потери данных при аварийных простоях системы.

Информация, связанная с данной

Управление журналами

Планирование резервного копирования для синхронного зеркального копирования:

Синхронное зеркальное копирование позволяет работать с FlashCopy для создания копии данных, сохраняемых на внешних накопителях IBM System Storage.

FlashCopy поддерживает создание синхронных копий. По завершении операции FlashCopy и исходный, и целевой тома готовы для работы с приложениями. FlashCopy можно использовать с другими технологиями IBM System Storage, такими как синхронное и глобальное зеркальное копирование, для создания синхронных копий данных на удаленном сайте, которые затем могут сохраняться с помощью стандартных способов резервного копирования. Перед использованием FlashCopy необходимо выполнить следующее:

- Определить исходные и целевые тома для взаимосвязей FlashCopy. Целевые тома FlashCopy следует распределить по рангам для лучшей производительности.
- Ознакомиться с требованиями к согласованности данных FlashCopy. В некоторых средах данные сохраняются в кэше системной памяти и только потом записываются на диск. Во избежание рассогласованности необходимо записать все данные исходного тома FlashCopy на диск перед выполнением операции FlashCopy.
- Существующий исходный том синхронного зеркального копирования может быть целевым томом FlashCopy. Это позволяет создать синхронную копию данных для целевого тома пары FlashCopy и затем скопировать эти данные на исходный том синхронного зеркального копирования в удаленном расположении.

Планирование производительности для синхронного зеркального копирования:

В этом разделе приведены сведения для настройки синхронного зеркального копирования, относящиеся к производительности.

Перед началом работы с синхронным зеркальным копированием следует принять во внимание следующие факторы:

- Исходный и целевой тома в зеркальном копировании должны иметь одинаковый тип памяти.
- Исходный и целевой логические тома должны иметь одинаковый объем, или целевой том должен быть больше.
- В среде зеркального копирования необходимо распределить нагрузку, чтобы обновления не приходились на небольшую группу томов в одном накопителе. Снижение производительности в целевой системе отрицательно скажется на производительности исходной системы.
- На производительность заметное влияние оказывает также число дисков, доступных приложению. Если дополнительная нагрузка приходится на ограниченное число дисков, то могут возрасти задержки, связанные с дисками, и в конечном счете снижаться производительность приложения. Это особенно важно в отношении временной памяти в системе, в которой настроены независимые пулы дисков. Вся временная память относится к пулу дисков SYSBAS. Если приложение не требует много временной памяти, то можно обойтись меньшим числом дисков в пуле SYSBAS. Учтите, что пул SYSBAS также обрабатывает запросы операционной системы и основных функций.

Информация, связанная с данной



Рекомендации по работе с функциями служб копирования в DS6000



Рекомендации по работе с функциями служб копирования в DS8000

| Планирование глобального зеркального копирования:

| Решения высокой готовности i5/OS поддерживают глобальное зеркальное копирование, которое
| обеспечивает высокую готовность и восстановление после сбоев в средах, в которых применяются
| устройства внешней памяти. Для применения этой технологии в решении высокой готовности необходимо
| соответствующее планирование.

| Технология глобального зеркального копирования IBM System Storage подразумевает, что все пользователи
| работают с одним зеркально защищенным соединением. Глобальное зеркальное копирование в решении

высокой готовности i5/OS возможно только тогда, когда в сеансе глобального зеркального копирования активен только один раздел System i™ на сервере System Storage. Никакие другие разделы System i или серверы на других платформах не могут применять глобальное зеркальное копирование в это же время. Если в сеансе глобального зеркального копирования участвует несколько пользователей, то результаты могут быть непредсказуемыми.

Если глобальное зеркальное копирование применяется на нескольких платформах, или если требуется реализовать глобальное зеркальное копирование на нескольких разделах System i, то можно использовать Службы копирования IBM для System i. Эта опция предлагается Lab Services.

Информация, связанная с данной



Рекомендации по работе с функциями служб копирования в DS6000



Рекомендации по работе с функциями служб копирования в DS8000

Требования к аппаратному обеспечению для глобального зеркального копирования:

Для настройки и управления решением высокой готовности i5/OS, которое использует технологию глобального зеркального копирования, убедитесь, что соблюдены минимальные требования к аппаратному обеспечению.

Для глобального зеркального копирования требуется соблюдение следующих минимальных требований к аппаратному обеспечению:

- Необходимы как минимум две модели System i, расположенные в разных местах, к каждой из которых подключен хотя бы один внешний накопитель IBM System Storage DS6000 или DS8000. Внешние накопители DS6000 и DS8000 поддерживаются для всех моделей System i, к которым возможно подключение внешней памяти по технологии Fibre Channel.
- Необходима одна из перечисленных моделей адаптеров Fibre Channel:
 - Контроллер дисков 2766 2 Gigabit Fibre Channel PCI
 - Контроллер дисков 2787 2 Gigabit Fibre Channel PCI-X
 - Контроллер дисков 5760 4 Gigabit Fibre Channel PCI-X
- Для поддержки внешнего загрузочного накопителя для DS6000 or DS8000 требуется новый процессор ввода-вывода:
 - Компонент 2847 PCI-X IOP для SAN
- Перед началом настройки необходимо соответствующим образом подготовить диски. Один набор дисков потребуется для источника, такой же набор - для целевого объекта, и по одному набору дисков для каждой копии, обеспечивающей согласованность данных.

Информация, связанная с данной



iSeries™ и IBM TotalStorage: Руководство по применению внешнего диска в системе i5



IBM System Storage DS6000 Information Center



IBM System Storage DS8000 Information Center

Требования к программному обеспечению для глобального зеркального копирования:

Перед настройкой решения высокой готовности i5/OS, которое использует глобальное зеркальное копирование, убедитесь, что соблюдены минимальные требования к программному обеспечению.

Минимальные требования глобального зеркального копирования к программному обеспечению таковы:

- Каждая модель System i в решении высокой готовности должна работать под управлением i5/OS V6R1, чтобы применялась лицензионная программа IBM System i High Availability Solutions Manager (iHASM) (5761-HAS).

Примечание: В предыдущих выпусках можно по-прежнему использовать Службы копирования IBM для System i, предлагаемые Lab Services, чтобы работать с решениями IBM System Storage. Если глобальное зеркальное копирование применяется на нескольких платформах, или если требуется реализовать глобальное зеркальное копирование на нескольких разделах System i, то также можно использовать Службы копирования IBM для System i.

- Лицензионный продукт IBM System i High Availability Solutions Manager(iHASM)–5761-HAS, установленный в каждой системе, участвующей в решении высокой готовности, которое использует глобальное зеркальное копирование.
- Лицензионная программа iHASM использует интерфейс командной строки памяти (DSCLI) для управления памятью. DSCLI является обязательным программным компонентом для всех решений IBM System Storage. DSCLI должен быть установлен во всех системах или разделах, участвующих в решении высокой готовности, в котором применяется любая из технологий IBM System Storage, такая как мгновенное копирование, синхронное зеркальное копирование или глобальное зеркальное копирование. Для применения DSCLI необходимо также наличие следующих компонентов:
 - Java версии 1.4
 - Компонент 35 (поставщик услуг шифрования CCA), установленный в системе или разделе
- Необходимо установить последние PTF.

Информация, связанная с данной

 iSeries™ и IBM TotalStorage: Руководство по применению внешнего диска в системе i5

 IBM System Storage DS6000 Information Center

 IBM System Storage DS8000 Information Center

Требования к средствам связи для глобального зеркального копирования:

Перед настройкой решения высокой готовности i5/OS, которое использует глобальное зеркальное копирование, убедитесь, что соблюдены минимальные требования к линиям связи.

Для использования технологии глобального зеркального копирования следует использовать или запланировать использование сети хранения данных (SAN).

SAN - это специализированная централизованная инфраструктура защиты информации, которая обеспечивает многоканальную связь между точками системы и устройствами хранения данных. Технология SAN применяется для решений на основе IBM System Storage, таких как внешние накопители DS8000 или DS6000.

Ниже приведены минимальные требования к средствам связи для решения высокой готовности i5/OS, использующего глобальное зеркальное копирование:

- Необходима одна из перечисленных моделей адаптеров Fibre Channel:
 - Контроллер дисков 2766 2 Gigabit Fibre Channel PCI
 - Контроллер дисков 2787 2 Gigabit Fibre Channel PCI-X
 - Контроллер дисков 5760 4 Gigabit Fibre Channel PCI-X
- Продукт System i поддерживает различные типы коммутаторов SAN. Полный список поддерживаемых коммутаторов приведен на Web-сайте Storage area network (SAN).
- Для повышения общей устойчивости и производительности рекомендуется воспользоваться функциями многоканального ввода-вывода. Многоканальный ввод-вывод позволяет применять несколько устройств Fibre Channel, подключенных к одним и тем же логическим дискам в накопителе. При правильной настройке это позволяет избежать сбоев при отказе отдельных устройств, блоков ввода-вывода или даже колец HSL. Многоканальный ввод-вывод также улучшает производительность за счет распределения нагрузки по доступным каналам. Каждое из альтернативных подключений дискового накопителя является

независимым. Наличие нескольких подключений улучшает устойчивость данных, допуская работу с дисковой памятью даже в случае сбоя одного из каналов.

Ссылки, связанные с данной



Web-сайт Storage area network (SAN)

Планирование ведения журнала для глобального зеркального копирования:

Ведение журнала играет важную роль в увеличении времени восстановления всех решений высокой готовности. В работе с технологиями на основе IBM System Storage, например, с глобальным зеркальным копированием, при ведении журнала выполняется принудительная запись на внешние накопители, поскольку зеркальное копирование происходит за пределами хранилища System i.

Журнал позволяет сохранить информацию о транзакциях в случае его аварийного выключения. Система заносит в журнал информацию обо всех изменениях объекта. Независимо от реализуемого решения высокой готовности ведение журнала является наилучшим способом предотвращения потери данных при аварийных простоях системы.

Информация, связанная с данной

Управление журналами

Планирование резервного копирования для глобального зеркального копирования:

Для создания синхронной копии данных при использовании технологии глобального зеркального копирования в решении высокой готовности используйте FlashCopy.

FlashCopy поддерживает создание синхронных копий. По завершении операции FlashCopy и исходный, и целевой тома готовы для работы с приложениями. FlashCopy можно использовать с другими технологиями IBM System Storage, такими как синхронное и глобальное зеркальное копирование, для создания синхронных копий данных на удаленном сайте, которые затем могут сохраняться с помощью стандартных способов резервного копирования. Перед использованием FlashCopy необходимо выполнить следующее:

- Определить исходные и целевые тома для взаимосвязей FlashCopy. Целевые тома FlashCopy следует распределить по рангам для лучшей производительности.
- Ознакомиться с требованиями к согласованности данных FlashCopy. В некоторых средах данные сохраняются в кэше системной памяти и только потом записываются на диск. Во избежание рассогласованности необходимо записать все данные исходного тома FlashCopy на диск перед выполнением операции FlashCopy.

Планирование производительности для глобального зеркального копирования:

Перед настройкой глобального зеркального копирования ознакомьтесь со следующими рекомендациями относительно производительности.

Ознакомьтесь со следующими рекомендациями относительно производительности перед использованием синхронного зеркального копирования:

- Исходный и целевой тома в зеркальном копировании должны иметь одинаковый тип памяти.
- Исходный и целевой тома в зеркальном копировании должны иметь одинаковый тип памяти.
- Как и при любой другой конфигурации диска, количество дисковых накопителей, доступных приложению, может значительно влиять на его производительность. Дополнительная нагрузка на ограниченное число дисковых накопителей может привести к более длительному ожиданию дисков и намного более продолжительному времени их ответа на запросы приложения. Это, в частности, важно, когда речь идет о временном хранилище в системе с независимыми пулами дисков. Все содержимое временного хранилища записывается в пул дисков SYSBAS. Если приложение не использует достаточного объема временного хранилища, то можно уменьшить число дисков в пуле дисков SYSBAS. Также необходимо помнить, что операционная система и базовые функции работают в пуле дисков SYSBAS.

Информация, связанная с данной



Рекомендации по работе с функциями служб копирования в DS6000



Рекомендации по работе с функциями служб копирования в DS8000

Планирование логической репликации

Логической репликацией называется поддержка нескольких экземпляров данных. Данные копируются с главного узла домена восстановления на резервные узлы. Если главный узел выйдет из строя, точка доступа будет перенесена на один из резервных узлов.

Логической репликацией называется процесс непрерывного копирования объектов в реальном времени. Объекты копируются с одного узла кластера на заранее выбранные другие узлы. Логическая репликация позволяет хранить несколько идентичных экземпляров объектов на разных узлах. Изменения, внесенные в объект на одном из узлов, автоматически реплицируются на другие узлы.

Необходимо выбрать программное обеспечение для логической репликации. Для репликации данных можно воспользоваться следующими программными средствами:

- **Продукты деловых партнеров IBM**

Деловые партнеры фирмы IBM по разработке кластерных продуктов предлагают специализированное программное обеспечение для репликации данных в кластере.

- **Пользовательские программы репликации**

Стандартные средства управления журналами, поставляемые фирмой IBM, позволяют сохранить данные об операциях, выполненных над объектами системы. Эти данные могут успешно использоваться для логической репликации.

Информация, связанная с данной

Управление журналами

Выбор систем для логической репликации:

При выборе систем для логической репликации необходимо учесть некоторые важные факторы.

Эти факторы следующие:

- Производительность
- Объем памяти
- Важность данных
- Защита на случай стихийных бедствий

На случай автоматического переноса ресурсов всегда полезно знать, какие данные и приложения расположены на главном и резервном узлах. Наиболее важные данные следует расположить на узле, который позволит обеспечить максимальную производительность в случае автоматического переноса ресурсов. На этом узле должно быть достаточно свободной памяти. Если главная система прекратит работу из-за недостатка памяти, после переноса ресурсов на резервном узле также может оказаться недостаточно памяти. На случай полного уничтожения вашего офиса стихийными бедствиями (наводнения, ураганы и тому подобное) рекомендуется расположить резервную систему в физически удаленном месте.

Партнеры IBM по разработке кластерных приложений и кластерные продукты:

Наряду с решением IBM можно приобрести промежуточное программное обеспечение для кластера от делового партнера обеспечения высокой готовности, которое применяет технологию логической репликации.

Также партнеры фирмы IBM по разработке кластерных продуктов предлагают специализированные средства для репликации данных и управления кластерами. Большинство решений от деловых партнеров основаны на логической репликации. Логическая репликация обеспечивает копирование объектов и запись

- | изменений в реальном времени. Объекты копируются с одного узла кластера на заранее выбранные другие узлы. Репликация позволяет хранить несколько идентичных экземпляров объектов на разных узлах.
- | Изменения, внесенные в объект на одном из узлов, автоматически реплицируются на другие узлы.

Планирование ведения журнала для логической репликации:

При использовании логической репликации необходимо использовать журнал для принудительной записи данных из рабочей копии в резервную.

Журнал позволяет сохранить информацию о транзакциях в случае его аварийного выключения. Система заносит в журнал информацию обо всех изменениях объекта. Независимо от реализуемого решения высокой готовности ведение журнала является наилучшим способом предотвращения потери данных при аварийных простоях системы.

В средах с логической репликацией ведение журнала является основой решения и как таковое требуется для реализации решения на основе этой технологии. При использовании логической репликации копирование данных в резервную систему в реальном времени может ограничиваться в соответствии с размером копируемого объекта. Например, программа обновляет запись, расположенную в файле, для которого ведется журнал. При этом она обновляет объект, например, пользовательское пространство, для которого не ведется журнал. Резервная копия становится полностью синхронизированной, когда все пользовательское пространство копируется в резервную систему. Если происходит сбой в главной системе, а объект пользовательского пространства еще не скопирован полностью, то потребуется вручную привести пользовательское пространство в то состояние, в котором оно находилось после последней успешной операции, при которой данные были скопированы полностью.

Информация, связанная с данной

Управление журналами

Планирование резервного копирования для логической репликации:

При использовании технологии логической репликации, реализованной в приложениях независимых поставщиков, необходимо запланировать резервное копирование для этой среды.

При логической репликации в резервную копию заносятся изменения в объектах, например в файлах или программах рабочей копии. Репликация происходит почти в реальном времени (одновременно). При ведении журнала для такого объекта, как файл, репликация проводится на уровне записи. Главным преимуществом этой технологии является возможность обращения операций резервного копирования к резервной копии в реальном времени. Для удаленного резервного копирования можно использовать резервную копию данных. При этом рабочая копия затронута не будет.

Планирование производительности для логической репликации:

При использовании технологии логической репликации в решении высокой готовности необходимо иметь представление о ее возможном влиянии на производительность этого решения.

При использовании логической репликации возможное влияние на производительность обусловлено латентностью процесса репликации. Это относится ко времени запаздывания, которое проходит между моментом, в который происходит изменение в исходной системе, и моментом, в который это изменение отражается в резервной системе. Синхронное ведение журнала помогает значительно снизить затраты времени. Независимо от используемого механизма передачи данных необходимо обеспечить надлежащую защиту передаваемого объема данных и правильно составить план линий связи и их скоростей для того чтобы среда могла работать с максимальными объемами копируемых данных. Объем требуемой переработки и латентность могут привести к сбоям в среде большого объема даже если средства передачи данных тщательно продуманы.

Планирование устойчивости среды

Устойчивость среды означает, что ваши объекты и атрибуты остаются согласованными в ресурсах, определенных в среде высокой готовности. Необходимо определить, какие ресурсы требуют наличия целостной среды для правильной работы, и создать административный домен, обеспечивающий согласованность атрибутов ресурсов в вашем решении высокой готовности.

Планирование домена управления кластером

Планирование домена управления кластером помогает оптимизировать управление синхронизируемыми ресурсами. Для того чтобы приложение успешно работало в любой системе в среде высокой готовности, необходимо определить, какие ресурсы будут необходимы приложению, в каких узлах кластера оно будет работать, и где будут храниться данные приложения.

Администратор кластера может создать домен управления кластером и добавить в него отслеживаемые ресурсы, синхронизируемые в узлах. Кластер i5/OS поддерживает список системных ресурсов, которые можно синхронизировать в пределах домена управления. Ресурсам в списке соответствуют записи отслеживаемых ресурсов (MRE).

При разработке домена управления кластером необходимо учитывать следующие факторы:

Какие узлы будут входить в домен управления кластером?

Определите, какими узлами кластера должен управлять домен управления кластером. Эти узлы соответствуют системам, в которых будет работать приложение или в которых будут храниться данные приложения. Для таких узлов необходима согласованная рабочая среда. Одни и те же узлы не могут входить в несколько доменов. Например, если кластер состоит из четырех узлов (Узел А, Узел В, Узел С и Узел D), то узлы А и В могут относиться к одному домену управления кластером, а узлы С и D - к другому. Однако узлы В и С нельзя добавить в третий домен, оставив их в прежнем домене.

Каким будет соглашение об именах для домена управления кластером?

В зависимости от размера и сложности кластерной среды может потребоваться установить стандартное соглашение об именах для равноправных CRG и доменов управления кластерами. Так как равноправная CRG создается вместе с доменом управления кластером, то, потребуется различать ее и CRG, представляющие домен управления. Например, равноправные CRG для доменов управления кластерами могут называться *ADMDMN1*, *ADMDMN2*, и так далее, а другие равноправные CRG - *PEER1* и так далее. Также для определения, используется ли какая-либо CRG в качестве домена управления кластером, можно воспользоваться API Показать информацию о группе ресурсов кластера (`QcstListClusterResourceGroupIn`). Равноправная CRG, соответствующая домену управления кластером, будет иметь другой идентификатор приложения, `QIBM.AdminDomain`.

Планирование записей отслеживаемых ресурсов (MRE)

Отслеживаемые ресурсы - это объекты i5/OS, которые можно определить в административном домене кластера. Эти ресурсы в среде высокой готовности должны оставаться согласованными в рамках всех систем; в ином случае во время простоя работа приложений может быть нарушена. Следует планировать, какие поддерживаемые ресурсы в данной среде следует отслеживать.

Следует определить, какие системные ресурсы требуется синхронизировать. Для каждого ресурса можно выбрать определенные атрибуты. Для правильной работы некоторых приложений, использующих несколько узлов, могут потребоваться специальные переменные среды. Более того, для работы с данными от нескольких узлов могут потребоваться определенные пользовательские профайлы. Также перед определением того, какими ресурсами следует управлять с помощью административного домена кластера, необходимо проверить соответствие приложений и данных требованиям операционной системы.

Планирование использования кластеров

Перед реализацией решения высокой готовности необходимо убедиться в том, что соблюдены все предварительные требования для работы с кластерами.

Требования к аппаратному обеспечению в кластере

Для реализации решения высокой готовности необходимо спланировать и настроить кластер. Кластер объединяет группу систем и ресурсов в среде высокой готовности.

Ниже перечислены минимальные требования к аппаратному обеспечению для кластеров:

- Необходимо наличие не менее двух моделей System i или логических разделов. В кластер может входить до 128 систем. Функции узла кластера может выполнять любая модель System i с операционной системой i5/OS версии V4R4M0 или выше.
- Для защиты от сбоев питания, приводящих к нарушению согласованности кластера, рекомендуется внешний источник бесперебойного питания.
- Кластеры применяют функции групповой рассылки протокола IP. Разные физические среды передачи данных по-разному приспособлены к групповой рассылке.
- Для работы с технологиями устойчивых данных, применяющими независимые пулы дисков, необходимо подобрать соответствующее аппаратное обеспечение. В случае сбоя защищенного диска могут применяться различные способы защиты от сбоев.

Понятия, связанные с данным

“Планирование устойчивости данных” на стр. 47

Устойчивость данных означает, что данные всегда доступны пользователям и приложениям.

Устойчивость данных обеспечивается применением технологий кластеров i5/OS с переносимыми дисками, распределенным зеркальным копированием или логической репликацией.

Ссылки, связанные с данной

“Таблица планирования для кластеров” на стр. 70

Перед настройкой кластера заполните эту таблицу, чтобы проверить, насколько подготовлена ваша рабочая среда.

Информация, связанная с данной

Источник бесперебойного питания

Многоадресные рассылки IP

Защита дисков

Требования к программному обеспечению в кластере

Для создания кластера требуется специальное программное обеспечение и лицензии.

1. Должна быть установлена система i5/OS V6R1.
2. Должен быть установлен компонент TCP/IP Connectivity Utilities.
3. Для использования технологий восстановления данных, таких как переключаемые диски или распределенная по сайтам зеркальная защита, должен быть выполнен ряд дополнительных требований.
4. Требуется компонент 41 (Переносимые ресурсы высокой готовности), если планируется работа со следующими интерфейсами:
 - Интерфейс управления кластерами System i Navigator

Примечание: Информация о работе с интерфейсом управления кластерами System i Navigator приведена в разделе Кластеры справочной системы Information Center продукта i5/OS V5R4.

- Лицензионная программа IBM System i High Availability Solutions Manager (iHASM). Эта лицензионная программа предоставляет несколько интерфейсов, для работы с которыми требуется компонент 41:
 - Графический интерфейс администратора решений высокой готовности
 - Графический интерфейс службы ресурсов кластера
 - Команды IBM System i High Availability Solutions Manager (iHASM)
 - API IBM System i High Availability Solutions Manager (iHASM)

Примечание:

5. Также можно использовать продукт делового партнера IBM или создать собственное приложение управления высокой готовностью, используя API кластера.

Понятия, связанные с данным

“Планирование переключаемых дисков” на стр. 48

Хранится только одна копия данных, которая размещена на переносимом аппаратном обеспечении - либо во внешнем блоке, либо в IOP логического раздела.

“Планирование распределенной по сайтам зеркальной защиты” на стр. 49

Распределенная по сайтам зеркальная защита обеспечивает несколько методик восстановления после аварии и обеспечения высокой готовности i5/OS: географическая зеркальная защита, синхронное зеркальное копирование и глобальное зеркальное копирование.

“Планирование устойчивости данных” на стр. 47

Устойчивость данных означает, что данные всегда доступны пользователям и приложениям.

Устойчивость данных обеспечивается применением технологий кластеров i5/OS с переносимыми дисками, распределенным зеркальным копированием или логической репликацией.

Ссылки, связанные с данной

“Таблица планирования для кластеров” на стр. 70

Перед настройкой кластера заполните эту таблицу, чтобы проверить, насколько подготовлена ваша рабочая среда.

Информация, связанная с данной

API кластеров

Требования к средствам связи в кластере

Кластер строится на любых средствах связи, поддерживающих протокол IP.

Служба ресурсов кластера работает на базе протоколов TCP/IP и UDP/IP. При этом поддерживается произвольное сочетание локальных сетей (LAN), глобальных сетей (WAN) и сетей OptiConnect (SAN). При выборе типа сети следует учитывать следующие факторы:

- Количество и объем транзакций
- Требования к быстродействию
- Физическое расстояние между узлами
- Цена

Если вы планируете создать резервные средства связи между узлами кластера, то при выборе типа сети для них следует руководствоваться теми же факторами. При проектировании кластера рекомендуется разместить часть резервных узлов в месте, физически изолированном от расположения основных узлов, на случай стихийных бедствий.

Для предотвращения возможных проблем с производительностью кластера при выборе типа сети следует учитывать объем информации, который планируется передавать между узлами. В настоящее время наиболее широкое распространение получили следующие типы сетей: Token-Ring, Ethernet, ATM, SPD OptiConnect, HSL OptiConnect и Virtual OptiConnect (высокоскоростное внутреннее соединение между логическими разделами).

HSL OptiConnect - это технология, реализованная на базе программного обеспечения OptiConnect for i5/OS (Компонент 23 i5/OS - i5/OS OptiConnect). Она применяется для создания сетей с высокой готовностью. HSL OptiConnect - это высокоскоростная системная сеть топологии точка-точка, связывающая отдельные узлы кластера по технологии HSL Loop. В сетях HSL OptiConnect применяется стандартный кабель HSL и не требуется дополнительное аппаратное обеспечение.

Для создания переносимого программного обеспечения, или CRG устойчивых устройств, вам потребуется переносимый диск. В среде с логическими разделами независимый ASP - это набор дисков, подключенных к общей шине нескольких логических разделов или к процессору ввода-вывода, выделенному пулу ввода-вывода. В среде с несколькими системами независимый ASP - это набор переносимых блоков

расширения, подключенных к тому же кольцу HSL, что и системы, входящие в соответствующий домен восстановления. В среде LPAR также могут применяться переносимые блоки расширения. .

Примечание: Если в вашей среде применяются адаптеры 2810, на которых настроен только протокол TCP/IP, а протоколы SNA и IPX не применяются, то в системе OS/400 версии V4R5M0 можно увеличить пропускную способность адаптеров путем указания опции Применять только для TCP(*YES) в описаниях соответствующих линий с помощью команды Работа с описаниями линии (WRKLIND). Эта опция автоматически применяется в OS/400 V5R1M0 и последующих версиях.

Понятия, связанные с данным

“Планирование переключаемых дисков” на стр. 48

Хранится только одна копия данных, которая размещена на переносимом аппаратном обеспечении - либо во внешней блоке, либо в IOP логического раздела.

Ссылки, связанные с данной

“Таблица планирования для кластеров” на стр. 70

Перед настройкой кластера заполните эту таблицу, чтобы проверить, насколько подготовлена ваша рабочая среда.

Организация выделенной сети для кластера:

При обычной работе базовый поток данных на кластере минимален. Тем не менее, настоятельно рекомендуется создать избыточные средства связи для каждого узла кластера.

| Средства связи считаются избыточными, если между любыми двумя узлами кластера есть по крайней мере
| две линии связи. При выходе любой линии из строя связь не будет прервана, и кластер не распадется. Однако
| следует иметь в виду, что если обе линии связи подключены к одному адаптеру, то узким местом становится
| адаптер. Еще стоит помнить, что не всегда можно избежать распада кластера. Кластер может распасться
| при перебоях в питании или аппаратном сбое системы. Если к каждому узлу будут подключены две линии
| связи, то одну из них можно выделить в исключительное использование кластера, а вторую отдать под
| прочие сетевые задачи и рассматривать как резервную линию на случай выхода выделенной линии из строя.
| Возникновения наиболее часто встречающихся предпосылок к распаду кластера можно избежать путем
| создания избыточных средств связи между узлами кластера.

Советы: Средства связи кластера:

При создании линий связи учтите следующие особенности.

- Пропускная способность линий связи должна быть достаточной для обычных потоков данных, а также для потоков данных кластера, включая его служебные потоки данных (например, пульс).
- Для повышения надежности не рекомендуется ограничиваться одной линией для связи нескольких узлов.
- Не следует перегружать линию связи, которая используется для контроля работоспособности узлов.
- По возможности следует устранить все узкие места - такие, в которых единичный сбой может привести к нарушению работы кластера. Например, не рекомендуется подключать несколько линий связи к одному адаптеру, одному процессору ввода-вывода или одному блоку расширения.
- При высокой нагрузке на основную сеть рекомендуется выделить отдельную сеть для репликации данных и контроля пульса.
- Для передачи служебной информации между узлами кластера лучше всего подходит функция групповой рассылки протокола UDP. Если физическая среда передачи данных поддерживает возможность групповой рассылки, то в пределах одной подсети узлы кластера смогут обмениваться служебной информацией в режиме групповой рассылки, что существенно снизит нагрузку на сеть. За пределы локальной сети сообщения всегда передаются в режиме точка-точка протокола UDP. Средства связи кластера реализованы таким образом, чтобы не зависеть от маршрутизации при рассылке групповых сообщений.
- Групповые сообщения нестабильны по своей природе. Частота передачи сообщений зависит от количества узлов в сети и сложности структуры управления кластером и может достигать 40 пакетов в секунду и

превышать это значение. Колебания частоты передачи сообщений могут отрицательно сказаться на устаревшем сетевом оборудовании. Например, применение агентов протокола SNMP, которым требуется анализ каждого группового пакета UDP, приводит к перегрузкам сети. Пропускной способности устаревшего сетевого оборудования может быть недостаточно для обработки таких потоков данных. При планировании создания кластера следует обязательно учесть дополнительную нагрузку в виде групповых пакетов UDP на вашу сеть, так как в противном случае кластер может снизить производительность сети в целом.

Планирование производительности для кластеров:

Для обеспечения максимальной эффективности служб кластера в различных рабочих средах предусмотрена возможность изменения параметров, влияющих на производительность кластера.

В большинстве случаев можно пользоваться значениями, предусмотренными по умолчанию. Если же значения по умолчанию не обеспечивают хорошую производительность в вашей среде, попробуйте изменить их. Предусмотрена возможность как базовой настройки, так и расширенной.

Базовая настройка

Базовая настройка позволяет выбрать один из трех predetermined наборов значений для времени ожидания сообщения и частоты пульса. Если выбран набор 2, то для частоты пульса и времени ожидания применяются стандартные значения. Если выбран набор 1, то пульс становится более редким, время ожидания для сообщений повышается. В этом режиме кластеру потребуется больше времени на обнаружение сетевых неполадок. Если выбран набор 3, то пульс становится более частым, время ожидания для сообщений сокращается. В этом режиме кластеру потребуется меньше времени на обнаружение сетевых неполадок.

Расширенная настройка

С помощью расширенной настройки можно настроить отдельные параметры, используя заданные диапазоны значений. Это позволяет добиться максимального соответствия параметров производительности условиям конкретной среды. Прежде, чем приступать к расширенной настройке, рекомендуется проконсультироваться со специалистом из сервисного центра фирмы IBM. Неудачный выбор значений отдельных параметров может привести к резкому снижению производительности.

Настраиваемые параметры связи кластера:

С помощью API QcstChgClusterResourceServices (Изменить службу ресурсов кластера) можно настраивать ряд параметров службы ресурсов кластера, влияющих на производительность, для достижения максимальной эффективности в конкретной среде.

Команда Изменить кластер (CHGCLU) позволяет изменить только базовые параметры производительности, тогда как API QcstChgClusterResourceServices предоставляет гораздо больше возможностей.

С помощью API QcstChgClusterResourceServices и команды Изменить конфигурацию кластера (CHGCLUCFG) можно изменить параметры кластера, связанные с производительностью. На базовом уровне можно выбрать один из predetermined наборов параметров. Если нужен расширенный уровень настройки, то с помощью того же API можно изменять значения параметров по отдельности. В этом случае рекомендуется проконсультироваться со специалистами фирмы IBM. Неудачное сочетание значений отдельных параметров может резко снизить производительность кластера.

Когда следует менять параметры, влияющие на производительность кластера

В команде CHGCLU и API QcstChgClusterResourceServices предусмотрены простые средства изменения параметров производительности, не требующие глубокого понимания принципов работы кластера. На

базовом уровне в основном изменения затрагивают чувствительность пульса и время ожидания для отправки сообщений. Предусмотрены следующие значения:

1 (Большое время ожидания/редкий пульс)

Пульс становится более редким, время ожидания для сообщений увеличивается. В этом режиме кластеру потребуется больше времени на обнаружение сетевых неполадок.

2 (Значения по умолчанию)

Для частоты пульса и времени ожидания применяются стандартные значения. Эта опция удобна для восстановления стандартной конфигурации параметров производительности кластера.

3 (Малое время ожидания/частый пульс)

Пульс становится более частым, время ожидания для сообщений сокращается. В этом режиме кластеру потребуется меньше времени на обнаружение сетевых неполадок.

В следующей таблице приведены экспериментальные результаты применения различных значений.

Примечание: Время указывается в формате минуты:секунды.

	1 (Низкая чувствительность)			2 (Значения по умолчанию)			3 (Высокая чувствительность)		
	Выявление неполадок пульса	Анализ	Всего	Выявление неполадок пульса	Анализ	Всего	Выявление неполадок пульса	Анализ	Всего
Одна подсеть	00:24	01:02	01:26	00:12	00:30	00:42	00:04	00:14	00:18
Несколько подсетей	00:24	08:30	08:54	00:12	04:14	04:26	00:04	02:02	02:06

При выборе частоты пульса и времени ожидания следует учитывать особенности нагрузки на сеть и физической среды передачи данных. В высокоскоростной и надежной среде передачи данных (например, когда все системы кластера подключены к одной шине OptiConnect) имеет смысл применять более чувствительную среду в целях ускорения автоматического переноса ресурсов. В такой ситуации лучше выбрать опцию 3. Если же в вашей среде применяется сильно нагруженная шина Ethernet пропускной способностью 10 Мбит/с, и применение стандартных значений приводит к периодическому переносу ресурсов из-за тайм-аутов, вызванных недостаточной пропускной способностью сети, то будет целесообразно выбрать опцию 1 для того, чтобы фильтровать временные увеличения времени отклика в моменты пиковой нагрузки на сеть.

С помощью API Изменить службу ресурсов кластера можно изменять отдельные параметры производительности. Например, предположим, что все узлы кластера подключены к шине OptiConnect. Можно значительно увеличить производительность системы передачи сообщений, увеличив размер фрагмента сообщения до 32500 байт (в соответствии со значением MTU Opticonnect, существенно превышающим стандартное значение в 1464 байта). За счет этого будет снижена фрагментация сообщений и сокращены издержки на их сборку-разборку. Разумеется, выигрыш от такого изменения будет зависеть от характера приложений, применяемых в кластере. Прочие параметры описаны в документации по API и могут применяться для регулировки системы передачи сообщений и скорости обнаружения распада кластера.

Ссылки, связанные с данной

API QcstChgClusterResourceServices

Информация, связанная с данной

Команда Изменить кластер (CHGCLU)

Изменение параметров службы ресурсов кластера:

Параметры, применяемые службой ресурсов кластера по умолчанию, вполне удовлетворительны в большинстве рабочих сред. Однако их можно изменить.

Параметры можно изменять следующими способами:

- Задать общий уровень производительности, наиболее соответствующий вашей среде.
- Задать конкретные значения для каждого параметра для более тонкой настройки.

В первом случае у вас есть возможность выбрать один из трех predetermined наборов значений параметров. Обычный набор, применяемый по умолчанию, подробно описан в разделе Контроль пульса.

Вторым способом изменения параметров следует пользоваться только после консультации со специалистом.

Подробные инструкции по применению обоих способов изменения параметров приведены в описании API Изменить службу ресурсов кластера (QcstChgClusterResourceServices).

Ссылки, связанные с данной

API QcstChgClusterResourceServices

Информация, связанная с данной

Контроль пульса

Планирование использования кластеров различных версий:

Процедура создания кластера, в который будут входить узлы с различными версиями кластера, требует некоторых дополнительных действий.

По умолчанию текущая версия кластера становится равной потенциальной версии первого узла. Это приемлемо, если создание кластера начинается с узла с минимальной версией. Однако если вам потребуется начать создание кластера с узла с максимальной версией, то в дальнейшем вы не сможете добавлять в кластер узлы предыдущей версии. Это ограничение можно обойти, если при создании кластера явно указать, что версия кластера должна быть предыдущей по отношению к потенциальной версии первого узла.

Примечание: При использовании лицензионной программы IBM System i High Availability Solutions Manager (iHASM) во всех системах кластера требуется V6R1.

Рассмотрим это на примере кластера, состоящего из двух узлов. В кластер входят следующие узлы:

ИД узла	Выпуск	Потенциальная версия кластера
Узел А	V5R4	5
Узел В	V6R1	6

Если начать создание кластера с узла В, то нужно явно указать, что в данный кластер будут входить узлы разных версий. Для этого нужно задать целевую версию кластера 2.

Планирование производительности для кластеров

Изменение кластера может повлиять на его производительность.

Для работы кластера ресурсы системы расходуются на контроль пульса, управление CRG и узлами кластера, а также обмен сообщениями между CRG и узлами кластера. После первоначальной настройки кластера снижение его производительности может произойти только в результате его изменения.

В обычной рабочей среде работа кластеров будет оказывать минимальное влияние на системы с кластерами.

Таблица планирования для кластеров

Перед настройкой кластера заполните эту таблицу, чтобы проверить, насколько подготовлена ваша рабочая среда.

Таблица 1. Таблица конфигурации TCP/IP для кластеров

Требования к TCP/IP	
—	Запустить протокол TCP/IP на всех узлах, которые будут включены в кластер (команда Запустить TCP/IP (STRTCP)).
—	Настроить циклический адрес TCP (127.0.0.1) и перевести его в Активное состояние. Состояние циклического адреса TCP/IP можно проверить с помощью команды Работа с состоянием сети TCP/IP (WRKTCPTS) на каждом узле кластера.
—	Проверить, что IP-адреса кластера находятся в состоянии Активны, выполнив команду Работа с состоянием сети TCP/IP (WRKTCPTS) на нужном узле.
—	<p>Проверить, что сервер INETD активен на всех узлах кластера либо с помощью команды STRTCPSVR *INETD, либо в IBM Systems Director Navigator for i5/OS с помощью следующих действий:</p> <ol style="list-style-type: none"> 1. В Web-браузере введите <code>http://mysystem:2001</code>, где <code>mysystem</code> - это имя хоста системы. 2. Войдите в систему по своему профайлу пользователя и паролю. 3. Выберите Сеть в Навигаторе IBM Systems Director для i5/OS. 4. На странице Приветствие выберите Серверы TCP/IP. 5. На странице Серверы TCP/IP выберите Серверы TCP/IP. Появится список доступных серверов TCP/IP. 6. В списке выберите INETD. 7. В меню Выбрать действие выберите Запустить. Состояние сервера изменится на Запущен. <p>Сервер INETD также можно запустить с помощью команды Запуск сервера TCP/IP (STRTCPSVR), указав параметр *INETD. О его наличии можно судить по наличию задания пользователь QTCP (QTOGINTD) в списке активных заданий узла.</p>
—	Проверить, что пользовательскому профайлу для INETD, указанному в файле /QIBM/ProdData/OS400/INETD/inetd.config, предоставлены только минимально необходимые права доступа. Если у данного профайла есть больше, чем минимальные права доступа, при запуске кластера произойдет сбой. По умолчанию в качестве пользовательского профайла для INETD указывается QUSER.
—	Проверить возможность связи и обмена дейтаграммами UDP для всех IP-адресов кластера. Это можно сделать с помощью команды PING с локальным IP-адресом и команды TRACEROUTE с сообщением UDP.
—	Проверить, что порты 5550 и 5551 не применяются другими приложениями. Эти порты зарезервированы для служб кластера IBM. Список занятых портов можно получить с помощью команды Работа с состоянием сети TCP/IP (WRKTCPTS). Порт 5550 открывается и находится в состоянии Занят с помощью кластера после запуска INETD.

Таблица 2. Таблица домена управления для кластеров

Служба ресурсов кластера - Замечания относительно интерфейса кластера	
—	Установите IBM System i High Availability Solutions Manager (лицензионная программа iHASM (5761-HAS)). На всех узлах кластера, входящих в решение высокой готовности, должен быть установлен действующий ключ лицензии.
—	Установить Компонент 41 (i5/OS - HA Switchable Resources). На всех узлах кластера, входящих в домен устройств, должен быть установлен действующий ключ лицензии.
—	Убедитесь, что запущены все серверы хоста. Это можно сделать с помощью команды STRHOSTSVR (Запустить сервер хоста): STRHOSTSVR SERVER(*ALL)

Если в кластере будут применяться перемещаемые устройства, то для них должны быть выполнены следующие требования:

Таблица 3. Таблица конфигурации устойчивых устройств для кластеров

Требования к устойчивым устройствам	
—	Установите IBM System i High Availability Solutions Manager (лицензионная программа iHASM (5761-HAS). На всех узлах кластера, входящих в решение высокой готовности, должен быть установлен действующий ключ лицензии.
—	Проверьте, что на всех узлах кластера, входящих в домен устройств, установлен Компонент 41 (HA Switchable Resources) и для него существует действующий ключ лицензии.
—	Для работы с функциями управления дисками следует настроить сервер сервисных средств (STS), доступ к DST и пользовательские профайлы. Дополнительная информация приведена в разделе Активация и доступ к дисковым накопителям.
—	<p>Если вы переключаете устойчивые устройства между логическими разделами системы и управляете логическими разделами без помощи НМС, включите поддержку Virtual OptiConnect в разделах. Управление этим продуктом осуществляется при входе в DST. Дополнительная информация приведена в разделе Virtual OptiConnect.</p> <p>Если для управления логическими разделами вы применяете Консоль аппаратного обеспечения, то измените свойства профайла раздела на вкладке OptiConnect и включите поддержку Virtual OptiConnect в каждом разделе в перемещаемой конфигурации. Для вступления изменения в силу активируйте профайл раздела.</p>
—	<p>Если блок расширения подключен к шине HSL OptiConnect и используется двумя системами, и в одной из этих систем есть логические разделы, то во всех логических разделах должна быть включена поддержка HSL OptiConnect. Если вы управляете логическими разделами без помощи НМС, то управление этим продуктом осуществляется при входе в DST.</p> <p>Если для управления логическими разделами вы применяете Консоль аппаратного обеспечения, то измените свойства профайла раздела на вкладке OptiConnect и включите поддержку HSL OptiConnect для каждого раздела в перемещаемой конфигурации. Для вступления изменения в силу активируйте профайл раздела.</p>
—	<p>Если вы переключаете устойчивые устройства между логическими разделами и управляете логическими разделами без помощи НМС, то вы должны настроить либо общую шину для разделов, либо пул ввода-вывода. В одном разделе шина должна быть настроена в режиме Владелец общей шины, а во всех остальных разделах, которые будут участвовать в переключении устройств, - в режиме Пользователь общей шины.</p> <p>Если вы применяете для управления логическими разделами Консоль аппаратного обеспечения, то настройте пул ввода-вывода, содержащий процессор ввода-вывода, адаптер ввода-вывода и все подключенные ресурсы. Этот пул дает возможность переключения независимого ASP между разделами. Этот пул ввода-вывода должен быть доступен каждому разделу. Дополнительная информация приведена в разделе Переносимость аппаратного обеспечения. Дополнительные сведения по требованиям к планированию аппаратного обеспечения переносимых устройств приведены в разделе Требования к аппаратному обеспечению переносимых устройств.</p>
—	После подключения блока расширения к шине HSL между двумя системами блок расширения должен быть настроен как переносимый. Дополнительная информация приведена в разделе Переносимость аппаратного обеспечения.
—	После подключения блока расширения к шине HSL нужно перезапустить все серверы, подключенные к этой шине.
—	Значение MTU для всех транзитных участков сети должно быть больше, чем размер фрагмента сообщений кластера. Значение MTU для IP-адреса кластера можно узнать с помощью команды Работа с состоянием сети TCP/IP (WRKTCPS) на соответствующем узле. Помимо этого, следует проверить значение MTU на всех транзитных участках линии связи. После запуска кластера будет проще уменьшить размер фрагмента сообщения, чем повсеместно увеличить значение MTU. Дополнительная информация о размере фрагмента сообщения приведена в разделе Настраиваемые параметры связи кластера. Текущие параметры производительности можно посмотреть посредством API Показать информацию службы ресурсов кластера (QcstRetrieveCRSInfo) и изменить с помощью API Изменить службу ресурсов кластера (QcstChgClusterResourceServices).
—	Для географической зеркальной защиты убедитесь, что оба узла связаны с различными именами сайта.

Таблица 4. Таблица конфигурации защиты для кластеров

Требования к защите	
—	Если ошибка возникает при попытке запустить удаленный узел, следует проверить значение атрибута ALWADDCLU (Разрешить добавление в кластер) на удаленном узле. Этому атрибуту должно быть присвоено значение *ANY или *RQSAUT, в зависимости от вашей среды. Для применения значения *RQSAUT на узле должны быть установлены i5/OS Компонент 34 (Диспетчер цифровых сертификатов) и продукт Поставщик услуг шифрования CCA (компонент 35). Дополнительная информация о сетевом атрибуте ALWADDCLU приведена в разделе Подготовка узла к добавлению в кластер.
—	Поддержка состояния пользовательского профайла для INETD, указанного в /QIBM/ProdData/OS400/INETD/inetd.config. Специальные права доступа *SECADM и *ALLOBJ не требуются. По умолчанию в качестве пользовательского профайла для INETD указывается QUSER.
—	Убедитесь, что на всех узлах кластера, с которых вызываются кластерные API, существует специальный пользовательский профайл для вызова этого API, и этому профайлу должны быть предоставлены права доступа *IOSYSCFG.
—	Убедитесь, что на всех узлах, входящих в домены восстановления CRG, существует специальный пользовательский профайл для выполнения программ выхода.

Таблица 5. Таблица конфигурации заданий для кластеров

Рекомендации по работе с заданиями	
—	Кластерные API запускают задания для выполнения ряда операций. Эти задания выполняются либо под управлением пользовательского профайла программы выхода, указанной при создании CRG, либо под управлением пользовательского профайла, вызвавшего данный API (только при включении CRG устойчивых устройств). Для подсистемы, с которой связана очередь заданий указанного пользовательского профайла, должно быть снято ограничение на число заданий (*NOMAX), поступающих из данной очереди.
—	Задания направляются в очередь, указанную в описании задания. В свою очередь, описание задания берется из пользовательского профайла, связанного с CRG. По умолчанию задания направляются в очередь QWATCH. Поскольку эта очередь интенсивно используется другими заданиями, ее применение может замедлить выполнение программ выхода. Рекомендуется создать специальную очередь заданий для выполнения кластерных программ выхода.
—	Задания программ выхода используют пул оперативной памяти и атрибуты выполнения, указанные в описании задания. По умолчанию задания будут выполняться в пуле, в котором выполняется большое число прочих заданий с приоритетом 50. Это может привести к снижению производительности заданий программ выхода. Подсистема, вызывающая задания программ выхода, должна помещать их в пул, который не используется другими заданиями. Кроме того, рекомендуется назначить заданиям программ выхода приоритет не ниже 15, чтобы они могли выполняться быстрее большинства других заданий.
—	Укажите системное значение QMLTTHDACN 1 или 2.

Для создания кластеров и работы с ними можно пользоваться разными интерфейсами. Один из них - это интерфейс Службы ресурсов кластера. Для применения Службы ресурсов кластера должны быть выполнены следующие условия.

Таблица 6. Таблица конфигурации Службы ресурсов кластера для кластеров

Замечания относительно графического интерфейса Службы ресурсов кластера	
—	Установите IBM System i High Availability Solutions Manager (лицензионная программа iHASM (5761-HAS)). На всех узлах кластера, входящих в решение высокой готовности, должен быть установлен действующий ключ лицензии.
—	Установить Компонент 41 (i5/OS - HA Switchable Resources). На всех узлах кластера, входящих в домен устройств, должен быть установлен действующий ключ лицензии.
—	Убедитесь, что запущены все серверы хоста. Это можно сделать с помощью команды STRHOSTSVR (Запустить сервер хоста): STRHOSTSVR SERVER(*ALL)

Планирование FlashCopy

FlashCopy может применяться как средство для сокращения времени простоя при резервном копировании в среде высокой готовности i5/OS, в которой используются внешние накопители IBM Systems Storage. Перед использованием FlashCopy необходимо обеспечить выполнение минимальных требований.

Требования к аппаратному обеспечению для FlashCopy

Для использования FlashCopy в решении высокой готовности i5/OS убедитесь, что удовлетворены минимальные требования к аппаратному обеспечению:

Для использования FlashCopy необходимо соблюсти следующие минимальные требования к аппаратному обеспечению:

- По меньшей мере две модели или два логических раздела System i, разделенных географически по меньшей мере одним блоком внешней памяти IBM System Storage DS6000 или DS8000, подсоединенным к каждой системе. Блоки внешней памяти DS6000 и DS8000 поддерживаются всеми моделями System i, которые поддерживают стандарт подсоединения внешней памяти Fibre-Channel.
- Необходима одна из перечисленных моделей адаптеров Fibre Channel:
 - Контроллер дисков 2766 2 Gigabit Fibre Channel PCI
 - Контроллер дисков 2787 2 Gigabit Fibre Channel PCI-X
 - Контроллер дисков 5760 4 Gigabit Fibre Channel PCI-X
- Перед началом настройки необходимо соответствующим образом подготовить диски. Один набор дисков потребуется для источника, такой же набор - для целевого объекта, и по одному набору дисков для каждой копии, обеспечивающей согласованность данных.

Требования FlashCopy к программному обеспечению

Для использования FlashCopy в решении высокой готовности для операционной системы i5/OS программное обеспечение должно отвечать определенным минимальным требованиям.

Минимальные требования FlashCopy к программному обеспечению таковы:

- Каждая модель System i в решении высокой готовности должна работать под управлением i5/OS V6R1, чтобы применялась лицензионная программа IBM System i High Availability Solutions Manager (iHASM) (5761-HAS).

Примечание: В предыдущих выпусках можно по-прежнему использовать Службы копирования IBM для System i, предлагаемые Lab Services, чтобы работать с решениями IBM System Storage. Если глобальное зеркальное копирование применяется на нескольких платформах, или если требуется реализовать глобальное зеркальное копирование на нескольких разделах System i, то также можно использовать Службы копирования IBM для System i.

- Наличие IBM System i High Availability Solutions Manager (iHASM) в каждой системе.
- Необходимо установить последние ПТФ.

Требования к средствам связи для FlashCopy

Вставьте сюда краткое описание; используется для первого абзаца и аннотации.

Для использования FlashCopy необходимо соблюсти следующие минимальные требования к средствам связи:

- Необходимы как минимум две модели System i, расположенные в разных местах, к каждой из которых подключен хотя бы один внешний накопитель IBM System Storage DS6000 или DS8000. Внешние накопители DS6000 и DS8000 поддерживаются для всех моделей System i, к которым возможно подключение внешней памяти по технологии Fibre Channel.
- Необходима одна из перечисленных моделей адаптеров Fibre Channel:
 - Контроллер дисков 2766 2 Gigabit Fibre Channel PCI
 - Контроллер дисков 2787 2 Gigabit Fibre Channel PCI-X

- | — Контроллер дисков 5760 4 Gigabit Fibre Channel PCI-X
- Для поддержки внешнего загрузочного накопителя для DS6000 or DS8000 требуется новый процессор ввода-вывода:
 - Компонент 2847 PCI-X IOP для SAN
- Перед началом настройки необходимо соответствующим образом подготовить диски. Один набор дисков потребуется для источника, такой же набор - для целевого объекта, и по одному набору дисков для каждой копии, обеспечивающей согласованность данных.

Планирование защиты для высокой готовности

Перед настройкой решения высокой готовности следует еще раз оценить текущие стратегии защиты в среде и внести необходимые изменения для обеспечения высокой готовности.

Рассылка информации по кластеру

Объяснение необходимости защиты рассылаемой по кластеру информации.

С помощью API Разослать информацию (QcstDistributeInformation) узлы домена восстановления могут обмениваться сообщениями. Эта возможность часто применяется в программах выхода. Применяя этот API, следует помнить, что данные передаются без шифрования. Поэтому данный API можно применять для рассылки конфиденциальной информации только в случае, если сеть защищена в целом.

Для рассылки временных данных и обмена ими можно пользоваться API хэш-таблиц кластера. Эти API хранят данные во временной памяти. Как только узел выходит из хэш-таблицы кластера, данные пропадают. Указанные API можно вызывать только с узлов, входящих в домен хэш-таблиц кластера. Кроме того, на узле должны быть запущены службы ресурсов кластера.

Прочая информация, передаваемая при обмене сообщениями в кластере, также не шифруется. Это относится и к низкоуровневым сообщениям. Если в программах выхода применяются стандартные средства обмена сообщениями, то следует помнить о том, что по сети передаются незашифрованные данные.

Замечания по применению кластеров с брандмауэрами

При создании кластеров в среде с брандмауэрами необходимо учитывать ряд ограничений и требований.

Если вы применяете кластеры вместе с брандмауэрами, то для каждого узла рекомендуется разрешить обмен исходящими и входящими сообщениями с другими узлами кластера. Такое "окно" в брандмауэре должно быть для каждого адреса кластера на каждом узле, чтобы он мог обмениваться данными со всеми остальными узлами кластера. По сети могут проходить различные типы пакетов IP. В кластерах используются пакеты ping (тип ICMP), UDP и TCP. При настройке брандмауэра вы можете фильтровать поток данных по типам. Для обеспечения нормальной работы кластеров с брандмауэрами следует разрешить пакеты ICMP, UDP и TCP. Для исходящего потока можно использовать любой порт, а для входящего - порты 5550 и 5551.

Управление пользовательскими профайлами на узлах кластера

Управлять пользовательскими профайлами на всех узлах кластера можно двумя способами.

- | В среде высокой готовности предполагается, что пользовательские профайлы с одинаковым именем
- | одинаковы во всех системах. Имя является уникальным идентификатором в кластере. Однако в
- | пользовательском профайле также содержится идентификатор пользователя (UID) и идентификатор группы
- | (GID). Для уменьшения числа внутренних операций в процессе принудительного переноса ресурсов, когда
- | доступ к независимому пулу дисков прекращается в одной системе и предоставляется в другой, следует
- | синхронизировать значения UID и GID в домене восстановления для CRG устройства. Существует два
- | способа синхронизации пользовательских профайлов в среде высокой готовности.

Первый способ заключается в создании домена управления кластером, отслеживающего общие ресурсы кластера. Кроме пользовательских профайлов, домен управления кластером позволяет отслеживать еще несколько типов общих ресурсов. Если домен управления кластером активен, то при обновлении

пользовательских профайлов изменения автоматически распространяются на остальные узлы. В противном случае изменения распространятся сразу после активизации домена управления кластером. Рекомендуется использовать этот метод, поскольку он автоматически обрабатывает пользовательские профайлы в среде высокой готовности.

Второй способ работы с пользовательскими профайлами - посредством Централизованного управления в System i Navigator. Эта возможность позволяет выполнять операции над несколькими системами и группами систем. С помощью Централизованного управления можно выполнять стандартные задачи оператора одновременно на нескольких узлах кластера. С помощью Централизованного управления можно применять функции для пользовательских профайлов к группам систем. Администратор может создать специальную команду синхронизации и выполнять ее всякий раз при создании нового профайла на одном из узлов.

Важное замечание:

- Если требуется сделать общими пользовательские профайлы, синхронизирующие пароли в пределах кластера, то установите значение системного параметра Сохранять идентификационные данные на сервере (QRETSVRSEC) равным 1.
- Если присвоить QRETSVRSEC значение 0 после добавления записи отслеживаемого ресурса (MRE) в пользовательский профайл, а затем сменить пароль, (если пароль отслеживается), то для MRE будет установлено общее состояние Несогласованная. MRE будет отмечена как непригодная для использования. Все изменения, внесенные после этого в пользовательский профайл, не будут синхронизированы. Для исправления этой неполадки присвойте QRETSVRSEC значение 1, удалите MRE и вновь добавьте MRE.

Задачи, связанные с данной

“Создание домена управления кластером” на стр. 101

В решении высокой готовности домен управления кластером обеспечивает механизм, синхронизирующий ресурсы в системах и разделах в кластере.

Настройка решения высокой готовности

Перед тем, как приступить к настройке решения высокой готовности в среде i5/OS, выполните соответствующие задачи планирования и ознакомьтесь с ресурсами и целями стратегии обеспечения высокой готовности и аварийного восстановления. В процессе создания собственного решения высокой готовности следует использовать существующие сценарии настройки высокой готовности и задачи, связанные с технологиями обеспечения высокой готовности.

Сценарии: Настройка высокой готовности

В сценариях настройки приводятся примеры сред высокой готовности i5/OS и пошаговые задачи по настройке, которые помогают реализовать решение высокой готовности на основе потребностей и требований к устойчивости.

В данных сценариях содержится описание бизнес-целей в сфере высокой готовности и приводится график, иллюстрирующий ресурсы внутри решения высокой готовности. Каждый пример решения включает в себя пошаговые инструкции по установке и тестированию высокой готовности. Как бы то ни было, эти сведения не описывают все примеры конфигурации, и может потребоваться дополнительное тестирование высокой готовности.

Сценарий: Переносимость диска между логическими разделами

В этом сценарии описано решение высокой готовности i5/OS, использующее пулы дисков, которые являются переносимыми между двумя логическими разделами, расположенными в одной и той же системе.

| Обзор

| Логические разделы позволяют работать с системой i5/OS, как с несколькими независимыми системами. Это решение оптимальным образом подходит организаций, которые уже применяют логические разделы.

| В этом сценарии не описана настройка логических разделов.

| Цели

| Преимущества этого решения:

- | • Экономичное решение, использующее доступные ресурсы системы.
- | • Обеспечивает готовность бизнес-ресурсов во время плановых простоев.
- | • Обеспечивается готовность бизнес-ресурсов во время некоторых неплановых простоев, таких как сбой одного логического раздела.
- | • За счет применения одной копии данных сводится к минимуму число необходимых дисковых накопителей.
- | • Данные всегда остаются текущими; синхронизация не требуется.

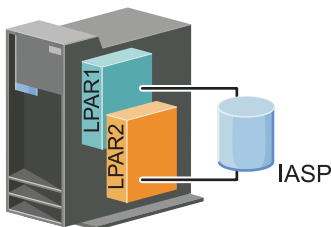
| Ограничения этого решения:

- | • Отсутствует процедура восстановления в случае сбоя на уровне всей среды.
- | • Требуется настроить логические разделы.
- | • Может потребоваться настроить избыточное аппаратное обеспечение между разделами.
- | • В независимом пуле дисков создается только одна логическая копия данных, которая может служить источником сбоев, хотя данные можно защитить с помощью технологии RAID.
- | • Запрещен параллельный доступ к пулу дисков из обоих логических разделов.

| Дополнительные сведения

| На этом изображении показана среда сценария:

|



|

| Этапы настройки

| Для настройки решения высокой готовности, описанного в этом сценарии, выполните следующие действия:

- | 1. Заполните справочную таблицу кластера
- | 2. Создайте кластер
- | 3. Добавьте узел
- | 4. Запустите узел
- | 5. Добавьте узел в домен устройств
- | 6. Создайте домен управления кластером
- | 7. Запустите домен управления кластером
- | 8. Создайте независимый пул дисков
- | 9. Добавьте записи отслеживаемых ресурсов
- | 10. Включите переносимость аппаратного обеспечения

- | 11. Создайте CRG устройств
- | 12. Запустите CRG устройств
- | 13. Добавьте пул дисков в число используемых
- | 14. Выполните принудительный перенос ресурсов для проверки работы решения высокой готовности

| **Сценарий: Совместное использование коммутлируемого диска системами**

| В данном сценарии описано решение высокой готовности i5/OS, использующее коммутлируемые диски в двух системах и обеспечивающее высокую готовность данных, приложений или устройств во время запланированных и незапланированных простоев.

| **Обзор**

| Благодаря технологии переключаемых дисков, обеспечивается простое решение высокой готовности. В этом решении одна копия, расположенная на переключаемом диске, всегда остается текущей. Такой подход позволяет отказаться от синхронизации данных между системами и исключает риск потери данных в ходе передачи.

| **Цели и задачи**

| Преимущества этого решения:

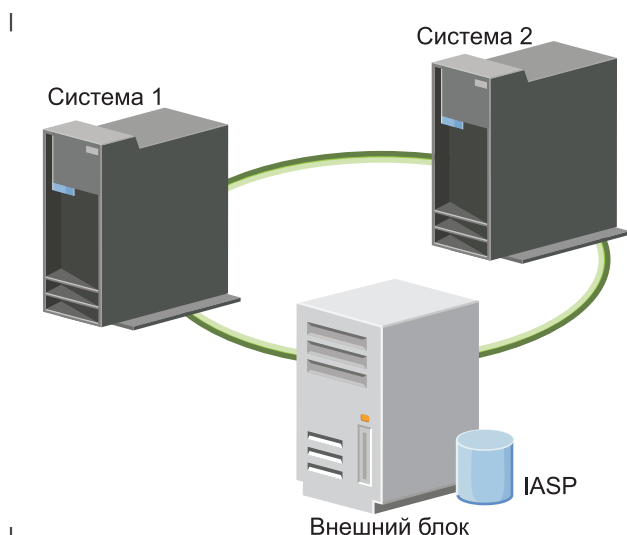
- | • Обеспечивается готовность бизнес-ресурсов во время плановых простоев
- | • Обеспечивается готовность бизнес-ресурсов во время unplanned простоев
- | • За счет применения одной копии данных сводится к минимуму число необходимых дисковых накопителей
- | • Минимальная дополнительная нагрузка
- | • Данные всегда остаются текущими; синхронизация не требуется

| Ограничения этого решения:

- | • Отсутствует процедура восстановления в случае сбоя на уровне всей среды
- | • В независимом пуле дисков создается только одна логическая копия данных, которая может служить источником сбоев, хотя данные можно защитить с помощью технологии RAID.
- | • Запрещен параллельный доступ к пулу дисков из обеих систем.

| **Дополнительные сведения**

| Данный график служит иллюстрацией к данному сценарию:



Действия по настройке

1. Заполните таблицу действий по планированию
2. Создайте кластер
3. Добавьте в кластер узел
4. Запустите узел
5. Добавьте узлы в домен устройств
6. Создайте домен управления кластером
7. Запустите домен управления кластером
8. Создайте независимый ASP
9. Добавьте записи отслеживаемых ресурсов
10. Сделайте аппаратное обеспечение расширенным
11. Создайте CRG устройства
12. Запустите CRG устройства
13. Добавьте ASP в число используемых
14. Выполните перенос ресурсов для проверки решения высокой готовности

Сценарий: Коммутируемый диск с географической зеркальной защитой

В данном сценарии описано решение высокой готовности i5/OS, использующее коммутируемые диски с географической зеркальной защитой в кластере с тремя узлами. Данное решение обеспечивает как восстановление после аварии, так и высокую готовность.

Обзор

В рабочей системе (Uptown) для переноса независимых пулов дисков между узлами используются переносимые диски. В решении также применяется географическая зеркальная защита для создания копии независимого пула дисков во второй системе (Downtown). Таким образом, это решение обеспечивает и восстановление после аварии, и высокую готовность. Преимущества этого решения, по существу, аналогичны преимуществам базового решения с переносимыми дисками, к которым добавлена возможность восстановления данных приложений после аварии посредством дублирования этих данных в другом расположении. Рабочая система (Uptown) содержит независимый пул дисков, который можно переносить между логическими разделами с целью обеспечения высокой готовности с минимальным временем принудительного переноса ресурсов во время плановых простоев (например, во время применения исправлений). Это решение также обеспечивает восстановление после аварии с помощью распределенной по сайтам и географической зеркальной защиты.

Географическая зеркальная защита является дополнительной функцией распределенной по сайтам зеркальной защиты, в которой выполняется зеркальное копирование данных в копию независимого пула дисков в удаленном расположении. Данные из независимого пула дисков в рабочей системе (Uptown) зеркально копируются в независимый пул дисков в резервной системе (Downtown). Это решение является простой и более экономичной альтернативой решениям на основе внешней системы хранения, таким как глобальное зеркальное копирование и синхронное зеркальное копирование IBM System Storage. Однако географическая зеркальная защита не обеспечивает всех опций производительности, которые предлагаются устройствами внешней памяти.

Цели и задачи

- Это решение обладает следующими преимуществами:
- Обеспечение готовности бизнес-ресурсов во время запланированных простоев
 - Обеспечение готовности бизнес-ресурсов во время некоторых незапланированных простоев
 - Обеспечение готовности бизнес-ресурсов во время аварии всей системы
 - В каждой системе может существовать одна копия данных, что минимизирует необходимое число накопителей

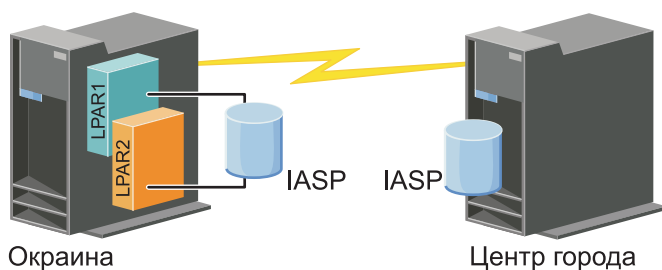
- Позволяет поддерживать актуальность данных без необходимости синхронизации

Ограничения этого решения:

- Отсутствует параллельный доступ к пулу дисков. Однако можно отсоединить зеркальную копию для автономного создания второй копии данных.
- Большое число ЦПУ, необходимое для поддержки географической зеркальной защиты, может влиять на быстродействие.
- Рассмотрите возможность использования резервных каналов связи и соответствующей пропускной способности.

Дополнительные сведения

Этот график иллюстрирует данное решение:



Действия по настройке

1. Заполните таблицу действий по планированию для кластеров
2. Создайте кластер
3. Добавьте в кластер узел
4. Запустите узел
5. Добавьте узел в домен устройств
6. Создайте CRG устройства
7. Определите имена сайтов
8. Создайте домен управления кластером
9. Запустите домен управления кластером
10. Создайте независимый ASP
11. Добавьте записи отслеживаемых ресурсов
12. Сделайте аппаратное обеспечение расширенным
13. Настройте географическую зеркальную защиту
14. Добавьте пулы дисков в число используемых
15. Выполните перенос ресурсов для проверки конфигурации

Задачи, связанные с данной

“Настройка географической зеркальной защиты” на стр. 110

Географическая зеркальная защита - это подфункция распределенной по сайтам зеркальной защиты. Для настройки решения высокой готовности с помощью географической зеркальной защиты необходимо настроить сеанс зеркальной защиты между рабочей и резервной системами.

Сценарий: Распределенная по сайтам зеркальная защита с географической зеркальной защитой

В данном сценарии описано решение высокой готовности i5/OS, использующее географическую зеркальную защиту в кластере с двумя узлами. Данное решение обеспечивает как восстановление после аварии, так и высокую готовность.

Обзор

Географическая зеркальная защита - это подфункция зеркальной защиты, распределенной по сайтам, которая осуществляет зеркальное копирование данных на удаленно расположенный независимый дисковый пул. Это решение предлагает аварийное восстановление в случае сбоя во всей рабочей системе (System 1). В такой ситуации произойдет переключение на резервную копию сайта (System 2), где можно будет продолжить работу с зеркальной копией данных. Это решение является простой и экономичной альтернативой использованию решений, базирующихся на внешней памяти, таких как Глобальное зеркальное копирование памяти IBM и Синхронное зеркальное копирование. Однако географическая зеркальная защита не предлагает всех опций производительности, которые предоставляют решения, использующие внешнюю память.

Цели

У этого решения есть следующие преимущества:

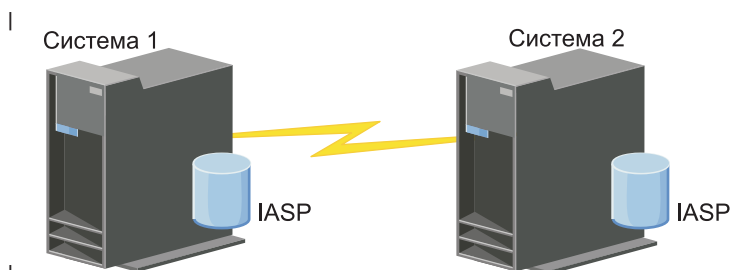
- Оно предполагает доступ к вашим бизнес-ресурсам во время запланированных отключений
- Предполагает доступ к бизнес-ресурсам во время незапланированных отключений
- Предполагает доступ к бизнес-ресурсам во время аварийных сбоев
- Предполагает возможность работы с оставшимися текущими данными и не требует синхронизации

У этого решения есть следующие ограничения:

- Не предусмотрен параллельный доступ к пулу дисков. Однако можно отсоединить зеркальную копию для работы со второй копией данных в автономном режиме.
- Потенциально влияет на производительность, поскольку для поддержки географической реальной защиты необходим центральный логический процессор (CPU).
- Учитывайте возможности дополнительных путей соединения и адекватную пропускную способность.

Дополнительные сведения

Следующий график иллюстрирует данное решение:



Действия по настройке

1. Заполните таблицу действий по планированию для кластеров
2. Создайте кластер
3. Добавьте узлы
4. Запустите узлы
5. Добавьте узлы в домен устройств
6. Создайте домен управления кластером
7. Запустите домен управления кластером
8. Создайте независимый ASP
9. Добавьте записи отслеживаемых ресурсов
10. Сделайте аппаратное обеспечение расширенным

- | 11. Создайте CRG устройства
- | 12. Запустите CRG устройства
- | 13. Добавьте ASP в число используемых
- | 14. Настройте географическую зеркальную защиту.
- | 15. Выполните перенос ресурсов для проверки конфигурации

| **Сценарий: Распределенная по сайтам зеркальная защита с синхронным зеркальным копированием**

| В данном сценарии описано решение высокой готовности i5/OS на основе внешних устройств памяти, обеспечивающее восстановление после аварий и высокую готовность системам, разделенным небольшими расстояниями. Синхронное зеркальное копирование - это решение IBM System Storage, синхронно копирующее данные из блока памяти рабочей системы в блок памяти резервной системы. Таким образом, данные в резервной системе остаются синхронизированными.

| **Обзор**

| Распределенная по сайтам зеркальная защита с синхронным зеркальным копированием обеспечивает высокую готовность и восстановление после аварий с помощью внешних блоков памяти, расположенных в пределах одного города. Независимый ASP копируется на внешних устройствах памяти, чтобы обеспечить готовность как в случае запланированных, так и незапланированных сбоев. Когда синхронное зеркальное копирование получает обновление рабочего тома с хоста, оно выполняет соответствующее обновление резервного тома. Синхронное зеркальное копирование функционирует на максимальном расстоянии 300 километров. Задержки в ответах при синхронном зеркальном копировании пропорциональны расстоянию между томами.

| В данном сценарии описана конфигурация стандартной технологии высокой готовности i5/OS. В нем не приведены инструкции по установке или настройке IBM System Storage серии DS6000 или DS8000. Здесь подразумевается, что решение IBM System Storage уже было установлено до настройки конфигурации высокой готовности i5/OS. Сведения об установке и настройке DS6000 приведены в IBM System Storage DS6000 Information Center. Сведения об установке и настройке DS8000 приведены в IBM System Storage DS8000 Information Center.

| **Цели и задачи**

| У этого решения есть следующие преимущества:

- | • Копирование полностью управляется внешним блоком памяти, и поэтому не используется CPU System i. Копирование продолжается в блоке памяти, даже если происходит системный сбой.
- | • Готовность бизнес-ресурсов при запланированных или незапланированных простоях, которые включают в себя техническое обслуживание или простои, связанные с программным обеспечением/PTF, а также восстановление после аварий.
- | • Отсутствие необходимости синхронизации ввода-вывода
- | • Быстрое восстановление при применении совместно с ведением журнала. С помощью журнала можно быстрее восстановить данные в случае непредвиденного сбоя или автоматического переноса ресурсов. С помощью функции ведения журнала изменения данных переносятся на диск, где осуществляется зеркальное копирование. Если не вести журнал, можно потерять данные, которые находятся в памяти. При ведении журнала можно восстановить транзакции на уровне данных, а также сократить время восстановления.
- | • Возможность использовать функцию FlashCopy на обоих направлениях синхронного зеркального копирования.

| У этого решения есть следующие ограничения:

- | • Оно требует внешнего аппаратного обеспечения памяти
- | • Рекомендуется использовать избыточные соединения и соответствующую пропускную способность

- Нет параллельного доступа к пулу дисков

Дополнительные сведения

Следующий график иллюстрирует данное решение:



Действия по настройке

1. Заполните таблицу действий по планированию для кластеров
2. Создайте кластер
3. Добавьте узлы
4. Запустите узлы
5. Добавьте узлы в домен устройств
6. Создайте домен управления кластером
7. Запустите домен управления кластером
8. Создайте независимый ASP
9. Добавьте записи отслеживаемых ресурсов
10. Сделайте аппаратное обеспечение расширенным
11. Создайте CRG устройства
12. Запустите CRG устройства
13. Добавьте ASP в число используемых
14. Настройте сеанс синхронного зеркального копирования
15. Выполните перенос ресурсов для проверки конфигурации

Сценарий: Распределенная по сайтам зеркальная защита с глобальным зеркальным копированием

В данном сценарии описано решение высокой готовности i5/OS на основе внешних устройств памяти, обеспечивающее восстановление после аварий и высокую готовность системам, разделенным большими расстояниями. Глобальное зеркальное копирование - это решение IBM Systems Storage, асинхронно копирующее данные из блока памяти рабочей системы в блок памяти резервной системы. Таким образом, данные в резервной системе остаются синхронизированными.

Обзор

Распределенная по сайтам зеркальная защита с глобальным зеркальным копированием обеспечивает восстановление после аварий с помощью внешних блоков памяти, несмотря на большую удаленность. Независимый ASP копируется на внешних устройствах памяти, чтобы обеспечить готовность как в случае запланированных, так и незапланированных сбоев.

В данном сценарии описана конфигурация стандартной технологии высокой готовности i5/OS. В нем не приведены инструкции по установке или настройке IBM System Storage серии DS6000 или DS8000. Здесь подразумевается, что решение IBM System Storage уже было установлено до настройки конфигурации высокой готовности i5/OS. Сведения об установке и настройке DS6000 приведены в IBM System Storage DS6000 Information Center. Сведения об установке и настройке DS8000 приведены в IBM System Storage DS8000 Information Center.

Цели

У этого решения есть следующие преимущества:

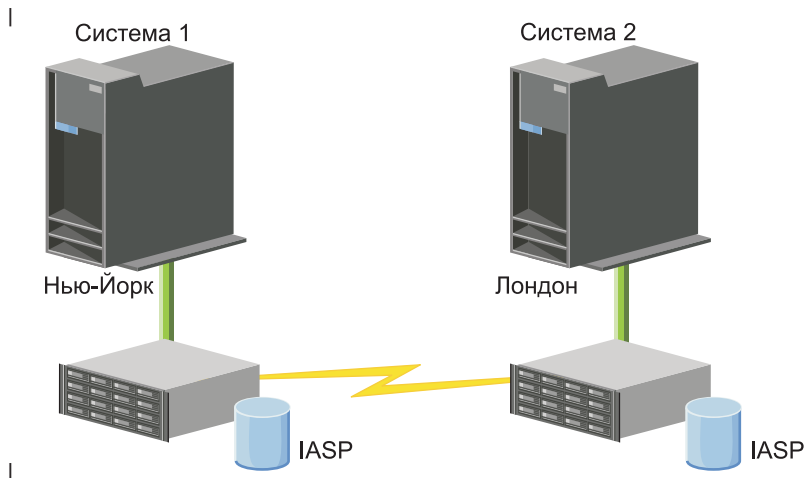
- Копирование полностью управляется внешним блоком памяти, и поэтому не используется CPU System i. Копирование продолжается в блоке памяти, даже если происходит системный сбой.
- Готовность бизнес-ресурсов при запланированных или незапланированных простоях, которые включают в себя техническое обслуживание или простои, связанные с программным обеспечением/PTF, а также восстановление после аварий.
- Быстрое восстановление при применении совместно с ведением журнала. С помощью журнала можно быстрее восстановить данные в случае непредвиденного сбоя или автоматического переноса ресурсов. С помощью функции ведения журнала изменения данных переносятся на диск, где осуществляется зеркальное копирование. Если не вести журнал, можно потерять данные, которые находятся в памяти. При ведении журнала можно восстановить транзакции на уровне данных, а также сократить время восстановления.
- Возможность использовать функцию FlashCopy на обоих направлениях глобального зеркального копирования.

У этого решения есть следующие ограничения:

- Оно требует внешнего аппаратного обеспечения памяти
- Рекомендуется использовать избыточные соединения и соответствующую пропускную способность
- Нет параллельного доступа к пулу дисков
- На сервере System Storage только в одном разделе System i может быть настроено глобальное зеркальное копирование. Никакие другие разделы System i или серверы из других платформ не могут использовать глобальное зеркальное копирование в тот же момент. Добавление более одного пользователя к сеансу глобального зеркального копирования может вызвать непредсказуемый результат.

Дополнительные сведения

Следующий график иллюстрирует данное решение:



Действия по настройке

1. Заполните таблицу действий по планированию для кластеров
2. Создайте кластер
3. Добавьте узлы
4. Запустите узлы
5. Добавьте узлы в домен устройств
6. Создайте домен управления кластером
7. Запустите домен управления кластером
8. Создайте независимый ASP
9. Добавьте записи отслеживаемых ресурсов
10. Сделайте аппаратное обеспечение расширенным
11. Создайте CRG устройства
12. Запустите CRG устройства
13. Добавьте ASP в число используемых
14. Настройте сеанс глобального зеркального копирования
15. Выполните перенос ресурсов для проверки конфигурации

Настройка TCP/IP для высокой готовности

Служба ресурсов кластера поддерживает только протокол IP, и поэтому все узлы кластера (системы и логические разделы в среде высокой готовности) должны быть доступны по протоколу IP. Это означает, что на всех узлах должны быть настроены интерфейсы IP.

Узлам должны быть назначены IP-адреса - администратор сети может сделать это вручную, создав таблицы маршрутов TCP/IP, либо автоматически с помощью специализированных протоколов. Таблица маршрутов TCP/IP - это аналог карты, по которой ведется поиск узлов. Каждому узлу должен быть присвоен уникальный IP-адрес.

Каждому узлу можно назначить до двух IP-адресов. Эти адреса не должны изменяться приложениями, не связанными с кластерами. При назначении IP-адресов запишите соответствие между адресами и линиями связи. Если по каким-либо причинам одна из линий будет более предпочтительна, чем другая, то предпочтительной линии следует назначить первый IP-адрес. Первый назначенный IP-адрес рассматривается

функцией работы с надежными сообщениями и средствами контроля пульса как предпочитаемый. Все IP-адреса каждого узла должны иметь возможность связи со всеми остальными IP-адресами кластера. Связь между адресами проверяется так: между адресами в обоих направлениях должен проходить пакет ping и сообщение trace протокола UDP.

Примечание: Для работы кластера необходимо, чтобы был активен циклический адрес (127.0.0.1). Этот адрес применяется для отправки сообщений локальному узлу и в большинстве случаев активизируется автоматически. Однако если по каким-либо причинам его работа будет прекращена, перестанет работать служба сообщений кластера.

Настройка атрибутов конфигурации TCP/IP

Для работы службы ресурсов кластера нужно, чтобы ряду атрибутов TCP/IP были присвоены определенные значения.

Эти атрибуты должны быть заданы до начала создания кластера:

- Если планируется применять сервер System i в качестве маршрутизатора между разными сетями, и на нем нет других протоколов маршрутизации, то необходимо присвоить опции пересылки IP-дейтаграмм значение *YES с помощью команды CHGTCPA (Изменить атрибуты TCP/IP).
- Запустите сервер INETD. Информация о запуске сервера INETD приведена в разделе “Запуск сервера INETD”.
- Присвойте параметру UDP CHECKSUM значение *YES с помощью команды CHGTCPA (Изменить атрибуты TCP/IP).
- Если в вашей сети установлены мосты между сетями Token-Ring, присвойте опции пересылки MCAST значение *YES.
- Если узлы кластера связаны с помощью OptiConnect for i5/OS, запустите подсистему QSOC с помощью команды STRSBS(QSOC/QSOC).

Запуск сервера INETD

Для выполнения любых операций на узле кластера должен быть запущен сервер INETD.

Рекомендуется, чтобы этот сервер всегда был запущен на всех узлах кластера.

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите **Сеть** в Навигаторе IBM Systems Director для i5/OS.
4. На странице Приветствие выберите **Серверы TCP/IP**.
5. На странице Серверы TCP/IP выберите **Серверы TCP/IP**. Появится список доступных серверов TCP/IP.
6. В списке выберите **INETD**.
7. В меню **Выбрать действие** выберите **Запустить**. Состояние сервера изменится на **Запущен**.

Сервер INETD также можно запустить с помощью команды Запуск сервера TCP/IP (STRTCPSVR), указав параметр *INETD. После запуска сервера INETD в списке активных заданий должно появиться задание Пользователь QTCP (QTOGINTD).

Ссылки, связанные с данной

Команда Запустить сервер TCP/IP (STRTCPSVR)

Настройка кластеров

Для любой реализации высокой готовности в i5/OS необходим настроенный кластер, который будет управлять устойчивыми ресурсами. При применении с другими технологиями устойчивости данных, например, коммутируемым диском, распределенной по сайтам зеркальной защитой или логическим копированием, технология кластеров обеспечивает ключевую инфраструктуру, необходимую для решений высокой готовности.

Служба ресурсов кластера состоит из компонентов, контролирующих топологию кластера, следящих за пульсом, а также предоставляющих возможность создания конфигурации кластера и групп ресурсов и работы с этими объектами. Кроме того, служба ресурсов кластера содержит функцию передачи надежных сообщений, которая позволяет следить за состоянием узлов кластера и синхронизировать информацию о состоянии ресурсов кластера на всех узлах. Графический пользовательский интерфейс Службы ресурсов кластера, являющийся частью IBM System i High Availability Solutions Manager (iHASM) лицензионный номер программы (5761-HAS), позволяет настраивать и управлять кластерами в рамках решения высокой готовности. Также лицензионная программа включает набор команд CL, позволяющих работать с конфигурациями кластеров.

Провайдеры приложений и пользователи могут использовать API и другие функции для расширения готовности приложения.

В дополнение к этим технологиям IBM деловые партнеры в сфере высокой готовности предоставляют приложения, использующие кластеры с технологией логического копирования.

Создание кластера

Процесс создания кластера начинается с настройки первого узла.

Для настройки остальных узлов кластера этот узел должен быть доступен администратору. Полный список требований для создания кластера приведен в разделе “Таблица планирования для кластеров” на стр. 70.

- | Для применения в кластере расширенных устройств или настройки решения высокой готовности с помощью
- | распределенной по сайтам зеркальной защиты должен быть выполнен ряд дополнительных условий.
- | Несколько примеров настройки решений высокой готовности, использующих данные технологии, приведены
- | в разделе Сценарии: Настройки решений высокой готовности. В каждом сценарии есть последовательные
- | задачи по настройке и обзор тех сбоев, для которых применяется данное решение. С помощью данных
- | примеров можно настроить решение высокой готовности или осуществить пользовательскую настройку в
- | соответствии со своими потребностями.

Для создания кластера выполните следующие действия:

- | 1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
- | 2. Войдите в систему, указав пользовательский профайл и пароль.
- | 3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
- | 4. На странице Приветствие выберите **Создать кластер**.
- | 5. Следуйте указаниям мастера Создание кластера.

После того, как кластер создан, страница Приветствия изменится и в верхней части страницы появится имя кластера. На этой странице перечислены несколько задач для работы с кластерами.

После создания кластера необходимо добавить дополнительные узлы и создать группы ресурсов кластера.

Информация, связанная с данной

Команда Создать кластер (CRTCLU)

API Создать кластер (QcstCreateCluster)

Подготовка узлов к добавлению в кластер:

Для того чтобы узел можно было добавить в кластер, нужно задать сетевой атрибут ALWADDCLU (Разрешить добавление в кластер).

Для этого нужно выполнить команду Изменить сетевые атрибуты (CHGNETA) на сервере, который будет узлом кластера. С помощью команды CHGNETA можно изменить сетевые атрибуты системы. Атрибут ALWADDCLU указывает, разрешено ли удаленным серверам включать данный сервер в свои кластеры.

Примечание: Для изменения значения атрибута ALWADDCLU нужны права доступа *IOSYSCFG.

Возможны следующие значения:

***SAME**

Значение не изменяется. Система поставляется с заранее установленным значением этого атрибута:
*NONE.

***NONE**

Другие системы не могут сделать данный сервер узлом кластера.

***ANY** Любая другая система может сделать данный сервер узлом кластера.

***RQSAUT**

Другая система может сделать данный узел узлом кластера при условии, что будет успешно выполнена идентификация этой системы.

Когда система получает запрос на добавление в кластер, она проверяет значение атрибута ALWADDCLU и выполняет одно из следующих действий: отклоняет запрос, разрешает добавить себя в кластер или запрашивает разрешение с помощью цифровых сертификатов X.509. *Цифровой сертификат* - это электронный аналог удостоверения личности, подлинность которого можно проверить. В случае, если установлен режим проверки, в локальной и удаленной системах должны быть установлены следующие продукты:

- i5/OS Компонент 34 (Диспетчер цифровых сертификатов)
- i5/OS Компонент 35 (Поставщик услуг шифрования CCA)

Если для ALWADDCLU указано значение *RQSAUT, то должен быть настроен список уполномоченных сертификатных компаний сервера защиты кластера i5/OS. Идентификатор сервера защиты кластера - QIBM_QCST_CLUSTER_SECURITY. В этот список нужно включить сертификатные компании, выдавшие сертификаты узлам, которым вы хотите разрешить добавление данной системы в кластер.

Добавление узлов:

Графический интерфейс Службы ресурсов кластера позволяет создавать простой кластер из двух узлов при первоначальном создании кластера. К кластеру в решении высокой готовности i5/OS можно добавить дополнительные узлы.

При создании нового кластера как части решения высокой готовности дополнительные узлы необходимо добавлять с помощью активного узла кластера.

Для добавления узла в кластер выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице **Службы ресурсов кластера** выберите задачу **Работа с узлами кластера**, чтобы просмотреть список узлов кластера.
5. На вкладке **Узлы** щелкните на меню **Выбрать действие** и выберите действие **Добавить узел**. Появится страница **Добавить узел**.
6. На странице **Добавить узел** укажите данные для нового узла. Нажмите кнопку **ОК** для добавления узла. Теперь новый узел появится в списке узлов. В кластере может быть до 128 узлов.

Запуск узлов:

Операция запуска узла кластера заключается в запуске кластера и службы ресурсов кластера на узле в среде высокой готовности i5/OS.

Узел может самостоятельно запустить службу ресурсов кластера и войти в кластер в случае, если ему удастся найти хотя бы один узел, уже входящий в кластер.

Для запуска узла выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На вкладке **Узлы** выберите узел, который требуется запустить.
5. Откройте меню **Выбрать действие** выберите опцию **Пуск**. В результате запуска службы ресурсов кластера состояние узла должно измениться на Работает.

Добавление узла в домен устройств:

Домен устройств - множество узлов кластера, совместно использующих ресурсы устройств.

При реализации решения высокой готовности, в котором используются технологии на основе независимых пулов дисков, например переносимые диски или распределенная по сайтам зеркальная защита, необходимо, чтобы узел был членом домена устройств. После добавления узла в домен устройств можно создать CRG, в которой определен домен восстановления кластера. Все узлы, входящие в домен восстановления CRG устройства, должны входить в один и тот же домен устройств. Узел кластера может принадлежать только одному домену устройств.

Для создания доменов устройств и управления ими требуется компонент 41 i5/OS (HA Switchable Resources). На всех узлах кластера, входящих в домен устройств, должен быть установлен ключ лицензии.

Для добавления узла в домен устройств выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице Службы ресурсов кластера щелкните на задаче **Работа с узлами кластера** для просмотра списка узлов кластера.
5. На вкладке **Узлы** выберите узел, который требуется добавить в домен устройств.
6. В меню **Выбрать действие** выберите опцию **Свойства**.
7. В поле **Домен устройств** на вкладке **Кластеры** укажите имя домена устройств.

Создание групп ресурсов кластера (CRG):

Группы ресурсов кластера (CRG) управляют ресурсами высокой готовности, например, приложениями, данными и устройствами. Каждый тип CRG управляет определенным типом ресурсов в среде высокой готовности.

Графический интерфейс Службы ресурсов кластера позволяет создавать различные CRG для управления ресурсами высокой готовности. Каждый тип CRG может применяться отдельно или вместе с другими CRG. Возможно, есть отдельное бизнес-приложение, для которого требуется высокая готовность. После подключения приложения к высокой готовности, можно создавать CRG, чтобы облегчить управление готовностью данного приложения.

Если необходимо, чтобы только приложение, а не его данные, были доступны в случае сбоя, можно создать CRG приложения. Однако, если необходимо, чтобы были доступны и приложение, и данные, их можно хранить в независимом ASP, определенном в CRG устройства. В случае сбоя весь независимый ASP переносится на резервный узел, обеспечивая доступность как приложения, так и его данных.

Создание CRG приложений:

Если в решении высокой готовности есть приложения, которым необходимо обладать высокой готовностью, можно создать группу ресурсов кластера приложения (CRG) для управления переносом ресурсов для этого приложения.

При создании CRG приложения можно разрешить использование активного устойчивого IP-адреса. Запуск CRG приложения с поддержкой активного устойчивого IP-адреса будет успешным.

Для создания CRG приложения выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профиль и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице Служба ресурсов кластера выберите **Работа с группами ресурсов кластера**, чтобы просмотреть список групп ресурсов кластера.
5. На странице Служба ресурсов кластера щелкните на меню **Выбрать действие**.
6. Выберите **Создать CRG приложения** и нажмите кнопку **Выполнить**. Будет показана страница Создание CRG приложения:
7. На странице **Общие сведения** укажите следующие сведения о CRG приложения:
 - В поле **Имя** укажите имя CRG. Имя должно состоять не более чем из 10 символов.
 - В поле **Устойчивый IP-адрес** укажите IP-адрес, который будет связан с CRG приложения. Это значение должно быть в десятичном формате и состоять не более чем из 15 символов. Устойчивый IP-адрес позволяет получить доступ к приложению вне зависимости от того, в какой системе в данный момент выполняется приложение. Поле **Настроить устойчивый IP-адрес** определяет, отвечает ли за создание IP-адреса пользователь или Служба ресурсов кластера.
 - В поле **Описание** введите описание CRG. Описание должно состоять не более чем из 50 символов.
 - Выберите **Разрешить перезапуск** и укажите число попыток перепуска для CRG приложения. Эти значения определяют число попыток перезапуска приложения на одном узле до осуществления переноса ресурсов на резервный узел.
 - В поле **Настроить устойчивый IP-адрес** выберите, хотите ли вы, чтобы Служба ресурсов кластера или пользователь настраивали и управляли устойчивым IP-адресом для CRG приложений. Возможны следующие значения:

Служба ресурсов кластера

Если указать данное значение, устойчивый IP-адрес не должен существовать на каком-либо узле домена восстановления до создания CRG. Он создается на всех узлах домена восстановления. Если IP-адрес уже существует, то создание CRG приложения будет невозможно.

Пользователь

Если указать данное значение, прежде чем запустить CRG, устойчивый IP-адрес необходимо будет добавить во все главные и резервные узлы, определенные в домене восстановления.

- Выберите **Разрешить активный устойчивый IP-адрес**, чтобы разрешить IP-адресу быть активным, когда он связан с CRG приложения. Это поле действительно, только когда значение поля Настроить устойчивый IP-адрес - служба ресурсов кластера.
- В поле **Пользовательская очередь для распределенной информации** укажите имя пользовательской очереди для получения распределенной информации. Имя должно состоять не более чем из 10 символов. В поле **Библиотека** укажите имя библиотеки, содержащей пользовательскую очередь для получения распределенной информации. Библиотека не может называться *CURLIB, QTEMP или *LIBL. Имя должно состоять не более чем из 10 символов.

Примечание: Если оставить поле Пользовательская очередь для распределенной информации пустым, необходимо также оставить пустым поле Имя библиотеки, задать в поле Ожидание переноса ресурсов значение 0, также как и в поле Действие по умолчанию при переносе ресурсов.

- В поле **Очередь сообщений переноса ресурсов** укажите имя очереди сообщений для получения сообщений при переносе ресурсов для данной группы ресурсов кластера. Если значение данного поля задано, указанная очередь сообщений должна существовать во всех узлах кластера домена восстановления после завершения работы программы выхода. Очередь сообщений переноса ресурсов не может находиться в независимом ASP. В поле **Библиотека** укажите имя библиотеки, содержащей очередь сообщений для получения сообщения о переносе ресурсов. Библиотека не может называться *CURLIB, QTEMP или *LIBL.
- В поле **Время ожидания переноса ресурсов** укажите число минут ожидания ответа на сообщение о переносе ресурсов в очереди сообщений кластера. Возможные значения:

Не ожидать

Перенос ресурсов осуществляется без вмешательства пользователя.

Неограниченное время ожидания

Время ожидания, пока будет получен ответ на запрос переноса ресурсов, не ограничено.

число Укажите число минут ожидания ответа на запрос переноса ресурсов. Если ответ не получен в течение указанного числа минут, дальнейшие действия определяются значением поля Действие по умолчанию при переносе ресурсов.

- В поле **Действие по умолчанию при переносе ресурсов** укажите, что должен делать кластер, если в течение определенного времени ожидания переноса ресурсов не получен ответ на сообщение о переносе ресурсов в очереди сообщений кластера. В этом поле можно задать значение **Продолжать перенос ресурсов** или **Отменить перенос ресурсов**.

8. На странице **Программа выхода** можно указать сведения для программы выхода CRG. Программы выхода обязательны для всех типов CRG, кроме CRG устройств. Программы выхода вызываются в случае возникновения события CRG на уровне кластера и реагируют на это событие.
9. На странице **Домен восстановления** добавьте узлы в домен восстановления и укажите их роль в кластере.

Создание CRG данных:

Группы ресурсов кластера (CRG) данных используются главным образом с приложениями логического копирования, предлагаемыми несколькими бизнес-партнерами в сфере высокой готовности. При реализации решения высокой готовности на основе логического копирования можно создать CRG данных, чтобы облегчить копирование данных главным и резервным узлами.

Для создания CRG данных выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице Служба ресурсов кластера выберите **Работа с группами ресурсов кластера**, чтобы просмотреть список групп ресурсов кластера.
5. На странице Служба ресурсов кластера щелкните на меню **Выбрать действие**.
6. Выберите **Создать CRG данных** и нажмите кнопку **Выполнить**. Появится страница Создание CRG данных.
7. На странице **Общие сведения** укажите следующие сведения о CRG данных:
 - В поле **Имя** укажите имя CRG. Имя должно состоять не более чем из 10 символов.
 - В поле **Описание** введите описание CRG. Описание должно состоять не более чем из 50 символов.
 - В поле **Пользовательская очередь для распределенной информации** укажите имя пользовательской очереди для получения распределенной информации. Имя должно состоять не более чем из 10 символов. В поле **Библиотека** укажите имя библиотеки, содержащей пользовательскую очередь для получения распределенной информации. Библиотека не может называться *CURLIB, QTEMP или *LIBL. Имя должно состоять не более чем из 10 символов.

Примечание: Если оставить поле Пользовательская очередь для распределенной информации пустым, необходимо также оставить пустым поле Имя библиотеки, задать в поле Ожидание переноса ресурсов значение 0, также как и в поле Действие по умолчанию при переносе ресурсов.

- В поле **Очередь сообщений переноса ресурсов** укажите имя очереди сообщений для получения сообщений при переносе ресурсов для данной группы ресурсов кластера. Если значение данного поля задано, указанная очередь сообщений должна существовать во всех узлах кластера домена восстановления после завершения работы программы выхода. Очередь сообщений переноса ресурсов не может находиться в независимом ASP. В поле **Библиотека** укажите имя библиотеки, содержащей очередь сообщений для получения сообщения о переносе ресурсов. Библиотека не может называться *CURLIB, QTEMP или *LIBL.
- В поле **Время ожидания переноса ресурсов** укажите число минут ожидания ответа на сообщение о переносе ресурсов в очереди сообщений кластера. Возможные значения:

Не ожидать

Перенос ресурсов осуществляется без вмешательства пользователя.

Неограниченное время ожидания

Время ожидания, пока будет получен ответ на запрос переноса ресурсов, не ограничено.

число Укажите число минут ожидания ответа на запрос переноса ресурсов. Если ответ не получен в течение указанного числа минут, дальнейшие действия определяются значением поля Действие по умолчанию при переносе ресурсов.

8. На странице **Программа выхода** можно указать сведения для программы выхода CRG. Программы выхода обязательны для всех типов CRG, кроме CRG устройств. Программы выхода вызываются в случае возникновения события CRG на уровне кластера и реагируют на это событие.
9. На странице **Домен восстановления** добавьте узлы в домен восстановления и укажите их роль в кластере.

Создание CRG устройств:

Группа ресурсов кластера (CRG) устройства состоит из пула ресурсов аппаратного обеспечения, который может быть расширен до сущности. Для создания расширенных устройств в рамках решения высокой готовности узлы, использующие эти устройства, должны быть частью CRG устройства.

Прежде чем создать CRG устройства, добавьте все узлы, которые будут использовать расширенный ресурс, в домен устройства.

Для создания CRG устройства выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице Служба ресурсов кластера выберите **Работа с группами ресурсов кластера**, чтобы просмотреть список групп ресурсов кластера.
5. На странице Служба ресурсов кластера щелкните на меню **Выбрать действие**.
6. Выберите **Создать CRG устройства** и нажмите кнопку **Выполнить**. Появится мастер **Создание CRG устройства**. Задача **Создать CRG устройства** доступна, только если запущены все узлы домена восстановления.
7. Следуйте указаниям мастера **Создание CRG устройства**. С помощью данного мастера можно создать CRG устройства. Также можно создать либо независимый ASP, либо задать использование существующего пула дисков.

CRG устройства следит за тем, чтобы сведения ресурса аппаратного обеспечения были идентичны на всех узлах домена восстановления, а также следит за идентичностью имен ресурсов. Также можно настроить домен управления кластером, чтобы он хранил зарегистрированные атрибуты объектов конфигурации, которые могут включать в себя имена ресурсов, идентичные во всем домене управления кластером. При

| применении распределенной по сайтам зеркальной защиты необходимо создать отдельные CRG устройств для независимых ASP и других типов расширенных устройств на каждом сайте.

| *Создание равноправных CRG:*

| Для определения роли узлов в средах распределения нагрузки можно создать равноправную CRG.

| Для создания равноправной CRG в кластере выполните следующие действия:

- | 1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
- | 2. Войдите в систему, указав пользовательский профайл и пароль.
- | 3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
- | 4. На странице Служба ресурсов кластера выберите **Работа с группами ресурсов кластера**, чтобы просмотреть список групп ресурсов кластера.
- | 5. На странице Служба ресурсов кластера щелкните на меню **Выбрать действие**.
- | 6. Выберите **Создать равноправную CRG** и нажмите кнопку **Выполнить**. Появится страница Создание равноправной CRG.
- | 7. На странице **Общие сведения** укажите следующие сведения о равноправной CRG:
 - | • В поле **Имя** укажите имя CRG. Имя должно состоять не более чем из 10 символов.
 - | • В поле **Описание** введите описание CRG. Описание должно состоять не более чем из 50 символов.
 - | • В поле **ИД приложения** укажите идентификатор приложения для равноправных групп ресурсов кластера в формате *[производитель].[приложение]*. Например, MyCompany.MyApplication. Идентификатор должен состоять не более чем из 50 символов.
- | 8. На странице **Программа выхода** можно указать сведения для программы выхода CRG. Программы выхода обязательны для всех типов CRG, кроме CRG устройств. Программы выхода вызываются в случае возникновения события CRG на уровне кластера и реагируют на это событие.
- | 9. На странице **Домен восстановления** добавьте узлы в домен восстановления и укажите их роль в кластере.

Запуск CRG:

Запуск группы ресурсов кластера (CRG) предусматривает активацию поддержки кластеров в среде высокой готовности i5/OS.

Для запуска CRG выполните следующие действия:

- | 1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
- | 2. Войдите в систему, указав пользовательский профайл и пароль.
- | 3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
- | 4. На странице Служба ресурсов кластера выберите **Работа с группами ресурсов кластера**, чтобы просмотреть список групп ресурсов кластера.
- | 5. На вкладке **Группа ресурсов кластера** выберите имя CRG, которую требуется запустить.
- | 6. В меню **Выбрать действие** выберите **Запустить**. В столбце Состояние будет показано, что CRG запущена.

Информация, связанная с данной

Команда Запустить CRG (STRCRG)

API Создать CRG (CRTCRG)

Задание очередей сообщений

| Можно задать либо очередь сообщений кластера, либо очередь сообщений переноса ресурсов. С помощью этих очередей сообщений можно будет определить причины сбоя в среде высокой готовности i5/OS.

Очередь сообщений кластера используется сообщениями на уровне кластера и выдает одно сообщение, управляющее всеми группами ресурсов кластера, переносящими ресурсы на определенный узел. Очередь сообщений переноса ресурсов используется сообщениями на уровне группы ресурсов кластера и выдает одно сообщение на каждую группу, переносящую ресурсы.

Задание очереди сообщений кластера

Примечание: Настроить кластер для использования очереди сообщений кластера также можно, задав очередь сообщений при выполнении мастера Создание кластера.

Для задания очереди сообщений кластера выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице службы ресурсов кластера нажмите кнопку **Показать свойства кластера**.
5. На странице Свойства кластера нажмите кнопку **Очередь сообщений кластера**.
6. Для создания очереди сообщений кластера укажите следующую информацию:
 - В поле **Имя** укажите имя очереди сообщений для получения сообщений, имеющих отношение к автоматическому переносу ресурсов на уровне кластера или узла. Для переноса ресурсов на уровне узла отправляется одно сообщение, управляющее переносом всех групп ресурсов кластера с помощью одного и того же главного узла. Если перенос ресурсов группы осуществляется отдельно, отправляется одно сообщение, управляющее переносом ресурсов данной группы. Сообщение отправляется новому главному узлу. Если значение данного поля задано, указанная очередь сообщений должна существовать во всех узлах кластера при их запуске. Очередь сообщений не может находиться в независимом ASP.
 - В поле **Библиотека** укажите имя библиотеки, содержащей очередь сообщений для получения сообщения о переносе ресурсов. Библиотека не может называться *CURLIB, QTEMP, *LIBL, *USRLIBL, *ALL или *ALLUSR.
 - В поле **Время ожидания переноса ресурсов** выберите **Не ждать** или **Неограниченное время ожидания**, или укажите число минут ожидания ответа на сообщение о переносе ресурсов в очереди сообщений кластера.
 - В поле **Действие по умолчанию при переносе ресурсов** укажите действие, предпринимаемое Службой ресурсов кластера, когда время ответа на сообщение о переносе ресурсов превысило значение времени ожидания при переносе ресурсов. В этом поле можно задать значение **Продолжать перенос ресурсов** или **Отменить перенос ресурсов**.

Задание очереди сообщений переноса ресурсов

Для задания очереди сообщений переноса ресурсов выполните следующие действия:

1. В Web-браузере введите `http://mysystem:2001`, где mysystem - это имя хоста системы.
2. Войдите в систему по своему профайлу пользователя и паролю.
3. Выберите **Служба ресурсов кластера** в окне Навигатор IBM Systems Director для i5/OS.
4. На странице Служба ресурсов кластера выберите **Работа с группами ресурсов кластера**, чтобы просмотреть список групп ресурсов кластера.
5. Из списка групп ресурсов кластера выберите группу, с которой необходимо работать.
6. На странице Служба ресурсов кластера щелкните на меню **Выбрать действие** и выберите **Свойства**.
7. На странице Общие сведения введите следующие значения для задания очереди сообщений переноса ресурсов:
 - В поле **Очередь сообщений переноса ресурсов** укажите имя очереди сообщений для получения сообщений при переносе ресурсов для данной группы ресурсов кластера. Если значение данного поля

задано, указанная очередь сообщений должна существовать во всех узлах кластера домена восстановления после завершения работы программы выхода. Очередь сообщений переноса ресурсов не может находиться в независимом ASP.

- В поле **Библиотека** укажите имя библиотеки, содержащей очередь сообщений для получения сообщения о переносе ресурсов. Библиотека не может называться *CURLIB, QTEMP или *LIBL.
- В поле **Время ожидания переноса ресурсов** укажите число минут ожидания ответа на сообщение о переносе ресурсов в очереди сообщений переноса ресурсов. Также можно указать действие, предпринимаемое Службой ресурсов кластера, когда время ответа на сообщение о переносе ресурсов превысило указанное время ожидания при переносе ресурсов.

Перенос ресурсов

Перенос ресурсов может выполняться для тестирования решения высокой готовности или штатного выключения главного узла, например, для резервного копирования или запланированного обслуживания системы.

В результате переноса ресурсов текущий главный узел становится резервным узлом. Эти роли задаются в домене восстановления группы ресурсов кластера. При переносе роли узлов, определенные в домене восстановления, меняются следующим образом:

- Текущий главный узел становится последним резервным узлом.
- Текущий первый резервный узел становится главным узлом.
- Остальные резервные узлы сдвигаются в списке на одну позицию вверх.

Перенос можно выполнять только для CRG приложений, данных и устройств, находящихся в состоянии 'активна'.

Примечание: При переносе CRG устройств по соображениям производительности рекомендуется синхронизировать имена пользовательских профайлов, UID и GID. Административный домен кластера упрощает синхронизацию пользовательских профайлов.

Для принудительного переноса ресурса выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице Служба ресурсов кластера выберите **Работа с группами ресурсов кластера**, чтобы просмотреть список групп ресурсов кластера.
5. Выберите CRG, в которой требуется выполнить принудительный перенос ресурсов. Перенос возможен для CRG приложений, данных или устройств.
6. В меню **Выберите действие** выберите **Перенос**.
7. В окне подтверждения нажмите кнопку **Да**.

Выбранная группа ресурсов кластера будет перенесена в резервный узел. В столбце Состояние будет показано новое имя узла.

Понятия, связанные с данным

Домен управления кластером

Задачи, связанные с данной

“Настройка доменов управления кластером” на стр. 101

В среде высокой готовности приложению и рабочей среде необходима согласованность с узлами, участвующими в высокой готовности. Домен управления кластером является реализацией в i5/OS функции восстановления среды, обеспечивающей согласованность рабочей среды с узлами.

Информация, связанная с данной

Команда Изменить главный узел CRG (CHGCRGPRI)

API Выполнить принудительный перенос ресурсов (QcstInitiateSwitchOver)

Настройка узлов

Узлы - это системы или логические разделы, принимающие участие в решении высокой готовности i5/OS.

Существует несколько задач, связанных с настройкой узлов. С помощью мастера Создание кластера можно настроить простой кластер с двумя узлами. Можно добавить дополнительные узла, но не более 128. В зависимости от технологий, входящих в состав решения высокой готовности, может возникнуть необходимость выполнения дополнительных задач по настройке.

Запуск узлов:

Операция запуска узла кластера заключается в запуске кластера и службы ресурсов кластера на узле в среде высокой готовности i5/OS.

Узел может самостоятельно запустить службу ресурсов кластера и войти в кластер в случае, если ему удастся найти хотя бы один узел, уже входящий в кластер.

Для запуска узла выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На вкладке **Узлы** выберите узел, который требуется запустить.
5. Откройте меню **Выбрать действие** выберите опцию **Пуск**. В результате запуска службы ресурсов кластера состояние узла должно измениться на Работает.

Информация, связанная с данной

Команда Запустить узел кластера (STRCLUNOD)

API Запустить узел кластера (QcstStartClusterNode)

Подготовка узлов к добавлению в кластер:

Для того чтобы узел можно было добавить в кластер, нужно задать сетевой атрибут ALWADDCLU (Разрешить добавление в кластер).

Для этого нужно выполнить команду Изменить сетевые атрибуты (CHGNETA) на сервере, который будет узлом кластера. С помощью команды CHGNETA можно изменить сетевые атрибуты системы. Атрибут ALWADDCLU указывает, разрешено ли удаленным серверам включать данный сервер в свои кластеры.

Примечание: Для изменения значения атрибута ALWADDCLU нужны права доступа *IOSYSCFG.

Возможны следующие значения:

*SAME

Значение не изменяется. Система поставляется с заранее установленным значением этого атрибута: *NONE.

*NONE

Другие системы не могут сделать данный сервер узлом кластера.

*ANY Любая другая система может сделать данный сервер узлом кластера.

*RQSAUT

Другая система может сделать данный узел узлом кластера при условии, что будет успешно выполнена идентификация этой системы.

Когда система получает запрос на добавление в кластер, она проверяет значение атрибута ALWADDCLU и выполняет одно из следующих действий: отклоняет запрос, разрешает добавить себя в кластер или запрашивает разрешение с помощью цифровых сертификатов X.509. *Цифровой сертификат* - это электронный аналог удостоверения личности, подлинность которого можно проверить. В случае, если установлен режим проверки, в локальной и удаленной системах должны быть установлены следующие продукты:

- i5/OS Компонент 34 (Диспетчер цифровых сертификатов)
- i5/OS Компонент 35 (Поставщик услуг шифрования CCA)

Если для ALWADDCLU указано значение *RQSAUT, то должен быть настроен список уполномоченных сертификатных компаний сервера защиты кластера i5/OS. Идентификатор сервера защиты кластера - QIBM_QCST_CLUSTER_SECURITY. В этот список нужно включить сертификатные компании, выдавшие сертификаты узлам, которым вы хотите разрешить добавление данной системы в кластер.

Добавление узлов:

Графический интерфейс Службы ресурсов кластера позволяет создавать простой кластер из двух узлов при первоначальном создании кластера. К кластеру в решении высокой готовности i5/OS можно добавить дополнительные узлы.

При создании нового кластера как части решения высокой готовности дополнительные узлы необходимо добавлять с помощью активного узла кластера.

Для добавления узла в кластер выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профиль и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице **Службы ресурсов кластера** выберите задачу **Работа с узлами кластера**, чтобы просмотреть список узлов кластера.
5. На вкладке **Узлы** щелкните на меню **Выбрать действие** и выберите действие **Добавить узел**. Появится страница **Добавить узел**.
6. На странице **Добавить узел** укажите данные для нового узла. Нажмите кнопку **ОК** для добавления узла. Теперь новый узел появится в списке узлов. В кластере может быть до 128 узлов.

Информация, связанная с данной

Команда **Добавить запись узла кластера (ADDCLUNODE)**

API **Добавить запись узла кластера (QcstAddClusterNodeEntry)**

Добавление узла в домен устройств:

Домен устройств - множество узлов кластера, совместно использующих ресурсы устройств.

1. При реализации решения высокой готовности, в котором используются технологии на основе независимых пулов дисков, например переносимые диски или распределенная по сайтам зеркальная защита, необходимо, чтобы узел был членом домена устройств. После добавления узла в домен устройств можно создать CRG, в которой определен домен восстановления кластера. Все узлы, входящие в домен восстановления CRG устройства, должны входить в один и тот же домен устройств. Узел кластера может принадлежать только одному домену устройств.

Для создания доменов устройств и управления ими требуется компонент 41 i5/OS (HA Switchable Resources). На всех узлах кластера, входящих в домен устройств, должен быть установлен ключ лицензии.

Для добавления узла в домен устройств выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.

- | 2. Войдите в систему, указав пользовательский профайл и пароль.
- | 3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
- | 4. На странице Службы ресурсов кластера щелкните на задаче **Работа с узлами кластера** для просмотра списка узлов кластера.
- | 5. На вкладке **Узлы** выберите узел, который требуется добавить в домен устройств.
- | 6. В меню **Выбрать действие** выберите опцию **Свойства**.
- | 7. В поле **Домен устройств** на вкладке **Кластеры** укажите имя домена устройств.

Информация, связанная с данной

Команда Добавить запись домена устройств (ADDDEVDMNE)

API Добавить запись домена устройств (ADDDEVDMNE)

Настройка CRG

Группы ресурсов кластера (CRG) управляют ресурсами в среде высокой готовности i5/OS. Существует несколько задач, которые обеспечивают управление ресурсами высокой готовности с помощью CRG.

Запуск CRG:

Запуск группы ресурсов кластера (CRG) предусматривает активацию поддержки кластеров в среде высокой готовности i5/OS.

Для запуска CRG выполните следующие действия:

- | 1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
- | 2. Войдите в систему, указав пользовательский профайл и пароль.
- | 3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
- | 4. На странице Служба ресурсов кластера выберите **Работа с группами ресурсов кластера**, чтобы просмотреть список групп ресурсов кластера.
- | 5. На вкладке **Группа ресурсов кластера** выберите имя CRG, которую требуется запустить.
- | 6. В меню **Выбрать действие** выберите **Запустить**. В столбце Состояние будет показано, что CRG запущена.

Информация, связанная с данной

Команда Запустить CRG (STRCRG)

API Создать CRG (CRTCRG)

Создание групп ресурсов кластера (CRG):

| Группы ресурсов кластера (CRG) управляют ресурсами высокой готовности, например, приложениями, данными и устройствами. Каждый тип CRG управляет определенным типом ресурсов в среде высокой готовности.

| Графический интерфейс Службы ресурсов кластера позволяет создавать различные CRG для управления ресурсами высокой готовности. Каждый тип CRG может применяться отдельно или вместе с другими CRG. Возможно, есть отдельное бизнес-приложение, для которого требуется высокая готовность. После подключения приложения к высокой готовности, можно создавать CRG, чтобы облегчить управление готовностью данного приложения.

| Если необходимо, чтобы только приложение, а не его данные, были доступны в случае сбоя, можно создать CRG приложения. Однако, если необходимо, чтобы были доступны и приложение, и данные, их можно хранить в независимом ASP, определенном в CRG устройства. В случае сбоя весь независимый ASP переносится на резервный узел, обеспечивая доступность как приложения, так и его данных.

| *Создание CRG приложений:*

Если в решении высокой готовности есть приложения, которым необходимо обладать высокой готовностью, можно создать группу ресурсов кластера приложения (CRG) для управления переносом ресурсов для этого приложения.

При создании CRG приложения можно разрешить использование активного устойчивого IP-адреса. Запуск CRG приложения с поддержкой активного устойчивого IP-адреса будет успешным.

Для создания CRG приложения выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профиль и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице Служба ресурсов кластера выберите **Работа с группами ресурсов кластера**, чтобы просмотреть список групп ресурсов кластера.
5. На странице Служба ресурсов кластера щелкните на меню **Выбрать действие**.
6. Выберите **Создать CRG приложения** и нажмите кнопку **Выполнить**. Будет показана страница Создание CRG приложения:
7. На странице **Общие сведения** укажите следующие сведения о CRG приложения:
 - В поле **Имя** укажите имя CRG. Имя должно состоять не более чем из 10 символов.
 - В поле **Устойчивый IP-адрес** укажите IP-адрес, который будет связан с CRG приложения. Это значение должно быть в десятичном формате и состоять не более чем из 15 символов. Устойчивый IP-адрес позволяет получить доступ к приложению вне зависимости от того, в какой системе в данный момент выполняется приложение. Поле **Настроить устойчивый IP-адрес** определяет, отвечает ли за создание IP-адреса пользователь или Служба ресурсов кластера.
 - В поле **Описание** введите описание CRG. Описание должно состоять не более чем из 50 символов.
 - Выберите **Разрешить перезапуск** и укажите число попыток перепуска для CRG приложения. Эти значения определяют число попыток перезапуска приложения на одном узле до осуществления переноса ресурсов на резервный узел.
 - В поле **Настроить устойчивый IP-адрес** выберите, хотите ли вы, чтобы Служба ресурсов кластера или пользователь настраивали и управляли устойчивым IP-адресом для CRG приложений. Возможны следующие значения:

Служба ресурсов кластера

Если указать данное значение, устойчивый IP-адрес не должен существовать на каком-либо узле домена восстановления до создания CRG. Он создается на всех узлах домена восстановления. Если IP-адрес уже существует, то создание CRG приложения будет невозможно.

Пользователь

Если указать данное значение, прежде чем запустить CRG, устойчивый IP-адрес необходимо будет добавить во все главные и резервные узлы, определенные в домене восстановления.

- Выберите **Разрешить активный устойчивый IP-адрес**, чтобы разрешить IP-адресу быть активным, когда он связан с CRG приложения. Это поле действительно, только когда значение поля Настроить устойчивый IP-адрес - служба ресурсов кластера.
- В поле **Пользовательская очередь для распределенной информации** укажите имя пользовательской очереди для получения распределенной информации. Имя должно состоять не более чем из 10 символов. В поле **Библиотека** укажите имя библиотеки, содержащей пользовательскую очередь для получения распределенной информации. Библиотека не может называться *CURLIB, QTEMP или *LIBL. Имя должно состоять не более чем из 10 символов.

Примечание: Если оставить поле Пользовательская очередь для распределенной информации пустым, необходимо также оставить пустым поле Имя библиотеки, задать в поле Ожидание переноса ресурсов значение 0, также как и в поле Действие по умолчанию при переносе ресурсов.

- В поле **Очередь сообщений переноса ресурсов** укажите имя очереди сообщений для получения сообщений при переносе ресурсов для данной группы ресурсов кластера. Если значение данного поля задано, указанная очередь сообщений должна существовать во всех узлах кластера домена восстановления после завершения работы программы выхода. Очередь сообщений переноса ресурсов не может находиться в независимом ASP. В поле **Библиотека** укажите имя библиотеки, содержащей очередь сообщений для получения сообщения о переносе ресурсов. Библиотека не может называться *CURLIB, QTEMP или *LIBL.
- В поле **Время ожидания переноса ресурсов** укажите число минут ожидания ответа на сообщение о переносе ресурсов в очереди сообщений кластера. Возможные значения:

Не ожидать

Перенос ресурсов осуществляется без вмешательства пользователя.

Неограниченное время ожидания

Время ожидания, пока будет получен ответ на запрос переноса ресурсов, не ограничено.

число Укажите число минут ожидания ответа на запрос переноса ресурсов. Если ответ не получен в течение указанного числа минут, дальнейшие действия определяются значением поля Действие по умолчанию при переносе ресурсов.

- В поле **Действие по умолчанию при переносе ресурсов** укажите, что должен делать кластер, если в течение определенного времени ожидания переноса ресурсов не получен ответ на сообщение о переносе ресурсов в очереди сообщений кластера. В этом поле можно задать значение **Продолжать перенос ресурсов** или **Отменить перенос ресурсов**.

8. На странице **Программа выхода** можно указать сведения для программы выхода CRG. Программы выхода обязательны для всех типов CRG, кроме CRG устройств. Программы выхода вызываются в случае возникновения события CRG на уровне кластера и реагируют на это событие.

9. На странице **Домен восстановления** добавьте узлы в домен восстановления и укажите их роль в кластере.

Информация, связанная с данной

Команда Создать CRG (CRTCRG)

API Создать CRG (CRTCRG)

Создание CRG данных:

Группы ресурсов кластера (CRG) данных используются главным образом с приложениями логического копирования, предлагаемыми несколькими бизнес-партнерами в сфере высокой готовности. При реализации решения высокой готовности на основе логического копирования можно создать CRG данных, чтобы облегчить копирование данных главным и резервным узлами.

Для создания CRG данных выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице Служба ресурсов кластера выберите **Работа с группами ресурсов кластера**, чтобы просмотреть список групп ресурсов кластера.
5. На странице Служба ресурсов кластера щелкните на меню **Выбрать действие**.
6. Выберите **Создать CRG данных** и нажмите кнопку **Выполнить**. Появится страница Создание CRG данных.
7. На странице **Общие сведения** укажите следующие сведения о CRG данных:
 - В поле **Имя** укажите имя CRG. Имя должно состоять не более чем из 10 символов.
 - В поле **Описание** введите описание CRG. Описание должно состоять не более чем из 50 символов.
 - В поле **Пользовательская очередь для распределенной информации** укажите имя пользовательской очереди для получения распределенной информации. Имя должно состоять не более чем из 10 символов. В поле **Библиотека** укажите имя библиотеки, содержащей пользовательскую очередь для

получения распределенной информации. Библиотека не может называться *CURLIB, QTEMP или *LIBL. Имя должно состоять не более чем из 10 символов.

Примечание: Если оставить поле Пользовательская очередь для распределенной информации пустым, необходимо также оставить пустым поле Имя библиотеки, задать в поле Ожидание переноса ресурсов значение 0, также как и в поле Действие по умолчанию при переносе ресурсов.

- В поле **Очередь сообщений переноса ресурсов** укажите имя очереди сообщений для получения сообщений при переносе ресурсов для данной группы ресурсов кластера. Если значение данного поля задано, указанная очередь сообщений должна существовать во всех узлах кластера домена восстановления после завершения работы программы выхода. Очередь сообщений переноса ресурсов не может находиться в независимом ASP. В поле **Библиотека** укажите имя библиотеки, содержащей очередь сообщений для получения сообщения о переносе ресурсов. Библиотека не может называться *CURLIB, QTEMP или *LIBL.
- В поле **Время ожидания переноса ресурсов** укажите число минут ожидания ответа на сообщение о переносе ресурсов в очереди сообщений кластера. Возможные значения:

Не ожидать

Перенос ресурсов осуществляется без вмешательства пользователя.

Неограниченное время ожидания

Время ожидания, пока будет получен ответ на запрос переноса ресурсов, не ограничено.

число Укажите число минут ожидания ответа на запрос переноса ресурсов. Если ответ не получен в течение указанного числа минут, дальнейшие действия определяются значением поля Действие по умолчанию при переносе ресурсов.

8. На странице **Программа выхода** можно указать сведения для программы выхода CRG. Программы выхода обязательны для всех типов CRG, кроме CRG устройств. Программы выхода вызываются в случае возникновения события CRG на уровне кластера и реагируют на это событие.
9. На странице **Домен восстановления** добавьте узлы в домен восстановления и укажите их роль в кластере.

Информация, связанная с данной

Команда Создать CRG (CRTCRG)

API Создать CRG (CRTCRG)

Создание CRG устройств:

Группа ресурсов кластера (CRG) устройства состоит из пула ресурсов аппаратного обеспечения, который может быть расширен до сущности. Для создания расширенных устройств в рамках решения высокой готовности узлы, использующие эти устройства, должны быть частью CRG устройства.

Прежде чем создать CRG устройства, добавьте все узлы, которые будут использовать расширенный ресурс, в домен устройства.

Для создания CRG устройства выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице Служба ресурсов кластера выберите **Работа с группами ресурсов кластера**, чтобы просмотреть список групп ресурсов кластера.
5. На странице Служба ресурсов кластера щелкните на меню **Выбрать действие**.
6. Выберите **Создать CRG устройства** и нажмите кнопку **Выполнить**. Появится мастер **Создание CRG устройства**. Задача **Создать CRG устройства** доступна, только если запущены все узлы домена восстановления.

7. Следуйте указаниям мастера **Создание CRG устройства**. С помощью данного мастера можно создать CRG устройства. Также можно создать либо независимый ASP, либо задать использование существующего пула дисков.
- CRG устройства следит за тем, чтобы сведения ресурса аппаратного обеспечения были идентичны на всех узлах домена восстановления, а также следит за идентичностью имен ресурсов. Также можно настроить домен управления кластером, чтобы он хранил зарегистрированные атрибуты объектов конфигурации, которые могут включать в себя имена ресурсов, идентичные во всем домене управления кластером. При применении распределенной по сайтам зеркальной защиты необходимо создать отдельные CRG устройств для независимых ASP и других типов расширенных устройств на каждом сайте.
- Информация, связанная с данной**
- Команда Создать CRG (CRTCRG)
- API Создать CRG (CRTCRG)

Создание равноправных CRG:

Для определения роли узлов в средах распределения нагрузки можно создать равноправную CRG.

Для создания равноправной CRG в кластере выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профиль и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице Служба ресурсов кластера выберите **Работа с группами ресурсов кластера**, чтобы просмотреть список групп ресурсов кластера.
5. На странице Служба ресурсов кластера щелкните на меню **Выбрать действие**.
6. Выберите **Создать равноправную CRG** и нажмите кнопку **Выполнить**. Появится страница Создание равноправной CRG.
7. На странице **Общие сведения** укажите следующие сведения о равноправной CRG:
 - В поле **Имя** укажите имя CRG. Имя должно состоять не более чем из 10 символов.
 - В поле **Описание** введите описание CRG. Описание должно состоять не более чем из 50 символов.
 - В поле **ИД приложения** укажите идентификатор приложения для равноправных групп ресурсов кластера в формате `[производитель].[приложение]`. Например, `MyCompany.MyApplication`. Идентификатор должен состоять не более чем из 50 символов.
8. На странице **Программа выхода** можно указать сведения для программы выхода CRG. Программы выхода обязательны для всех типов CRG, кроме CRG устройств. Программы выхода вызываются в случае возникновения события CRG на уровне кластера и реагируют на это событие.
9. На странице **Домен восстановления** добавьте узлы в домен восстановления и укажите их роль в кластере.

Информация, связанная с данной

- Команда Создать CRG (CRTCRG)
- API Создать CRG (CRTCRG)

Настройка доменов управления кластером

В среде высокой готовности приложению и рабочей среде необходима согласованность с узлами, участвующими в высокой готовности. Домен управления кластером является реализацией в i5/OS функции восстановления среды, обеспечивающей согласованность рабочей среды с узлами.

Создание домена управления кластером:

В решении высокой готовности домен управления кластером обеспечивает механизм, синхронизирующий ресурсы в системах и разделах в кластере.

Для создания домена управления кластером пользователь должен иметь права доступа к *IOSYSCFG и профайлу пользователя QCLUSTER. Для администрирования домена управления кластером пользователь должен иметь права доступа к CRG, представляющей домен управления кластером, профайлу пользователя QCLUSTER и командам группы ресурсов кластера.

Для создания домена управления кластером выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице службы ресурсов кластера нажмите кнопку **Работа с доменами управления**, чтобы увидеть список доменов управления кластером данного кластера. Если не было настроено ни одного домена управления кластером, список будет пустым.
5. Во вкладке **Домен управления** выберите **Создать домен управления**.
6. На странице Создать домен управления укажите следующие сведения о домене управления кластером:
 - В поле **Имя** введите имя домена управления кластером. Имя должно состоять не более чем из 10 символов.
 - В поле **Кластер** показано имя кластера. Значение этого поля менять нельзя.
 - В поле **Опция синхронизации** укажите действия по синхронизации, когда узел присоединяется к домену управления кластером. Это поле включено, только если кластер относится к версии 6 или выше. Возможны следующие значения:

Опция Последние изменения (по умолчанию)

Выберите данную опцию, если необходимо применить все изменения отслеживаемых ресурсов к домену управления кластером. Последнее изменение отслеживаемого ресурса применяется к ресурсу на всех активных узлах.

Опция Активный домен

Выберите эту опцию, если изменения отслеживаемых ресурсов допускаются только на активных узлах. Изменения отслеживаемых ресурсов с неактивных узлов не принимаются во внимание при присоединении узла к домену управления кластером. Опция Активный домен не применяется к областям памяти сервера (*NWSSTG) или сетевым конфигурациям сервера (*NWSCFG). Синхронизация данных ресурсов всегда основана на последних сделанных изменениях.

- В списке **Узлы домена управления** выберите узлы, которые необходимо добавить к домену управления кластером, и выберите **Добавить**.

Понятия, связанные с данным

“Управление пользовательскими профайлами на узлах кластера” на стр. 74

Управлять пользовательскими профайлами на всех узлах кластера можно двумя способами.

Информация, связанная с данной

Команда Создать административный домен кластера (CRTCAD)

API Создать административный домен кластера (QcstCrtClusterAdminDomain)

Добавление узла в домен управления кластером:

В домен управления кластером как часть решения высокой готовности можно добавить дополнительные узлы.

Прежде чем добавить узел в домен управления кластером, убедитесь, что узел также является частью кластера, в котором находится домен управления кластером. Если это не так, вы не сможете добавить узел к домену управления кластером. Домен управления кластером не обязательно должен быть активен, но ресурсы не будут согласованы до тех пор, пока он не будет активирован.

При добавлении узла к домену управления кластером MRE домена копируются в добавляемый узел. Если отслеживаемый ресурс не существует в новом узле, он создается доменом управления кластером. Если же он уже существует в добавляемом узле, он синхронизируется с доменом управления кластером, если тот активен. То есть, значения атрибутов каждого отслеживаемого ресурса добавляемого узла изменяются, чтобы соответствовать глобальным значениям отслеживаемых ресурсов активного домена.

Для добавления узла в домен управления кластером выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профиль и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице службы ресурсов кластера нажмите кнопку **Работа с доменами управления**, чтобы увидеть список доменов управления кластером данного кластера.
5. На странице Домены управления выберите домен управления кластером.
6. В меню **Выбрать действие** выберите **Свойства**.
7. На странице **Свойства** из списка **Узлы домена управления** выберите узел, который необходимо добавить к домену управления кластером. Нажмите кнопку **Добавить**.

Информация, связанная с данной

Команда Добавить запись узла административного домена кластера (ADDCADNODE)
API Добавить узел в домен восстановления (QcstAddNodeToRcvyDomain)

Запуск административного домена кластера:

Административные домены кластера обеспечивают устойчивость ресурсов, входящих в состав решения высокой готовности i5/OS.

После запуска административный домен кластера применяет в активных узлах все изменения, которые были внесены в отслеживаемые ресурсы, пока административный домен кластера был недоступен.

Для запуска административного домена кластера выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профиль и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице Службы ресурсов кластера выберите **Работа с административными доменами** для просмотра списка административных доменов кластера.
5. На странице Домены управления выберите домен управления кластером.
6. В меню **Выбрать действие** выберите **Запустить**.

В столбце Состояние будет показано, что административный домен кластера запущен.

Понятия, связанные с данным

“Синхронизация отслеживаемых ресурсов”

Синхронизация отслеживаемых ресурсов выполняется после их изменения в узлах из административного домена кластера.

Информация, связанная с данной

Команда Запустить административный домен кластера (STRCAD)

Синхронизация отслеживаемых ресурсов:

Синхронизация отслеживаемых ресурсов выполняется после их изменения в узлах из административного домена кластера.

В процессе синхронизации административный домен кластера пытается изменить каждый ресурс, значения атрибутов которого не совпадают с глобальными значениями (если отсутствуют ожидающие изменения). Ожидающие изменения передаются на все активные узлы домена и применяются ко всем связанным ресурсам на этих узлах. После рассылки ожидающих изменений обновляется глобальное значение. Кроме того, в зависимости от результата операции изменения глобальное состояние каждого связанного ресурса изменяется на *согласован* или *не согласован*. Если ресурс успешно изменен на всех активных узлах, то для него указывается глобальное состояние *согласован*. В случае сбоя операции изменения на одном или нескольких узлах указывается глобальное состояние *не согласован*.

Если в период простоя административного домена кластера один и тот же ресурс был изменен на нескольких узлах, то в процессе синхронизации после запуска домена все изменения передаются на все активные узлы. Обратите внимание, что в ходе активации административного домена кластера не соблюдается порядок обработки ожидающих изменений. Если один и тот же ресурс был изменен на нескольких узлах кластера, пока административный домен кластера был выключен, то в ходе активации изменения обрабатываются в произвольном порядке.

Если узел добавляется в неактивный административный домен кластера (т.е. при запуске узла административный домен кластера был недоступен), то синхронизация отслеживаемых ресурсов откладывается до запуска административного домена.

Примечание: Административный домен кластера и связанная с ним программа выхода поставляются IBM. Их не следует изменять с помощью API QcstChangeClusterResourceGroup или команды Изменить группу ресурсов кластера (CHGCRG); в противном случае возникнут непредвиденные результаты.

При необходимости отслеживаемые ресурсы можно изменить после завершения работы узла кластера, входящего в состав административного домена кластера. В ходе очередного запуска узла изменения будут синхронизированы на уровне административного домена кластера. В процессе синхронизации административный домен кластера применяет на активных узлах все изменения из неактивного узла, если изменения не были внесены в активном домене, пока узел был недоступен. Изменения, внесенные в отслеживаемый ресурс в активном домене, применяются после изменений из неактивного узла. Другими словами, вне зависимости от состояния узла потеря изменений отслеживаемого ресурса исключена. Для управления синхронизацией предусмотрена отдельная опция.

Если требуется завершить узел кластера из административного домена кластера и запретить передачу изменений, вносимых в неактивный узел, в активный домен после запуска узла (например, для тестирования узла кластера), то перед завершением работы узла его необходимо удалить из CRG уровня административного домена.

Понятия, связанные с данным

Команда Удалить запись узла административного домена (RMVCADNODE)

Задачи, связанные с данной

“Запуск административного домена кластера” на стр. 103

Административные домены кластера обеспечивают устойчивость ресурсов, входящих в состав решения высокой готовности i5/OS.

Информация, связанная с данной

Команда Удалить запись узла CRG (RMVCRGNODE)

Добавление записей отслеживаемых ресурсов:

В домен управления кластером можно добавить записи отслеживаемых ресурсов. В них определены важные ресурсы для того, чтобы изменения вносимые в эти ресурсы действовали для всей среды высокой готовности.

Для добавления записи отслеживаемого ресурса выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. На странице службы ресурсов кластера нажмите кнопку **Работа с доменами управления**, чтобы увидеть список доменов управления кластером данного кластера.
4. На странице Домены управления щелкните на значке напротив домена управления кластером и выберите **Работа с типами отслеживаемых ресурсов**.
Примечание: Действие **Работа с типами отслеживаемых ресурсов** доступно, только если узел, с которым вы хотите работать, принадлежит домену управления кластером. Появится список типов отслеживаемых ресурсов.
5. В списке типов отслеживаемых ресурсов щелкните на значке напротив типа отслеживаемых ресурсов и выберите **Добавить запись отслеживаемого ресурса**. Появится страница Добавить запись отслеживаемого ресурса.
6. Выберите атрибуты записи, которые требуется отслеживать, и нажмите **ОК**. Если объект MRE находится в библиотеке, для данного объекта необходимо указать имя и библиотеку. Созданная запись отслеживаемого ресурса будет добавлена в список ресурсов, отслеживаемых доменом управления кластером. Изменения, вносимые в отслеживаемый ресурс, синхронизируются по всем активным узлам домена управления кластером, когда домен активен. По умолчанию отслеживаются все атрибуты, связанные с отслеживаемым типом ресурса. Однако, можно выбрать те атрибуты, которые будут отслеживаться.
Задачи, связанные с данной
“Выбор атрибутов, которые необходимо отслеживать” на стр. 136
После добавления записей отслеживаемых ресурсов можно выбрать атрибуты, связанные с тем ресурсом, который необходимо отслеживать с помощью домена управления кластером.
Информация, связанная с данной
Команда Добавить MRE административного домена (ADDCADMRE)
API Добавить запись отслеживаемого ресурса (QfpadAddMonitoredResourceEntry)

Настройка коммутируемых дисков

Коммутируемые диски - это независимые ASP, которые были настроены как часть кластера i5/OS. Коммутируемые диски позволяют переносить данные и приложения, хранимые в независимом ASP, в другую систему.

Создание независимого ASP

Для того чтобы создать независимый ASP, можно воспользоваться мастером Создание пула диска. Этот мастер поможет создать новый пул диска и добавить к нему дисковые накопители.

С помощью мастера Создание пула диска можно включить в набор устройств с проверкой четности ненастроенные дисковые накопители и запустить защиту устройств с проверкой четности и сжатие диска. При добавлении дисковых накопителей не помещайте дисковые накопители из одного набора устройств с проверкой четности в несколько пулов дисков, поскольку сбой одного набора устройств повлияет на несколько пулов дисков.

Для создания независимого ASP с помощью мастера Создание пула дисков в Навигаторе IBM Systems Director для i5/OS выполните следующие действия:

Примечание: Для работы с диском в Навигаторе IBM Systems Director для i5/OS необходим соответствующий пароль конфигурации для Специальных сервисных средств.

Навигатор IBM Systems Director для i5/OS

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите **Настройка и службы** в окне Навигатора IBM Systems Director для i5/OS.

4. Выберите **Дисковые накопители**.
5. В меню **Выбор действий** выберите **Создать пул дисков**.
6. Следуя инструкциям мастера, добавьте дисковые накопители к новому пулу дисков.
7. Распечатайте конфигурацию диска, чтобы она была доступна в случае, если придется осуществлять восстановление.
8. Запишите взаимосвязь между именем и номером независимого ASP.

Навигатор System i

Для создания независимого ASP с помощью мастера Создание пула дисков в System i Navigator выполните следующие действия:

1. В System i Navigator разверните **Соединения** (либо активную среду).
2. Разверните систему, с которой вы хотите ознакомиться, а затем - **Настройка и службы** → **Аппаратное обеспечение** → **Дисковые накопители**.
3. Щелкните правой кнопкой мыши на списке **Пулы дисков** и выберите **Создать пул дисков**.
4. Следуя инструкциям мастера, добавьте дисковые накопители к новому пулу дисков.
5. Распечатайте конфигурацию диска, чтобы она была доступна в случае, если придется осуществлять восстановление.
6. Запишите взаимосвязь между именем и номером независимого ASP.

Примечание: После полной перезагрузки системы добавьте независимые ASP. Если необходимо использовать мастер Создание пула дисков в режиме Специальные сервисные средства (DST), после полной перезагрузки системы создайте связанное описание устройства для независимого ASP. Для создания описания устройства воспользуйтесь командой Создать описание устройства (ASP) (CRTDEVASP). Назовите описание устройства и ресурс так же, как и независимый ASP. С помощью команды Работа с описаниями устройств (WRKDEVVD) проверьте, что описание устройства и имя независимого ASP совпадают.

Включение зеркальной защиты

С помощью мастеров Добавить диск и Создать пул дисков можно в пошаговом режиме добавить пары дисков близкой емкости в защищенный пул дисков. После настройки дисков можно включить зеркальную защиту.

Зеркальная защита работает в пределах одной системы и отличается от распределенной по сайтам зеркальной защиты. В недоступном независимом пуле дисков зеркальную защиту можно запустить после перезапуска системы. В случае остальных пулов дисков перед включением зеркальной защиты необходимо перезапустить систему до Специальных сервисных средств (DST).

| Для того чтобы включить зеркальную защиту с помощью IBM Systems Director Navigator for i5/OS, выполните следующие действия:

- | 1. Выберите **Настройка и обслуживание** в окне IBM Systems Director Navigator for i5/OS.
- | 2. Выберите **Пулы дисков**.
- | 3. Выберите пул дисков для включения зеркальной защиты.
- | 4. В меню **Выбрать действие** выберите **Включить зеркальную защиту**.

| Для того чтобы включить зеркальную защиту с помощью System i Navigator, выполните следующие действия:

1. В окне System i Navigator разверните запись **Мои соединения** (или активную среду).
2. Разверните систему System i и выберите **Настройка и обслуживание** → **Аппаратное обеспечение** → **Диски** → **Пулы дисков**.
3. Щелкните правой кнопкой мыши на нужных пулах дисков и выберите **Включить зеркальную защиту**.

Выключение зеркальной защиты

- | При выключении зеркальной защиты один из накопителей каждой зеркальной пары становится ненастроенным. Перед выключением зеркальной защиты пула дисков убедитесь, что в каждой зеркальной паре присутствует по крайней мере один активный диск.
- | Конкретный диск зеркальной пары для удаления из конфигурации можно указать предварительно выключив его. Если диски не выключены, то система выбирает один из них автоматически.
- | В недоступном независимом пуле дисков зеркальную защиту можно выключить после перезапуска системы.
- | В случае остальных пулов дисков перед выключением зеркальной защиты необходимо перезапустить систему до Специальных сервисных средств (DST).
- | Зеркальная защита работает в пределах одной системы и отличается от распределенной по сайтам зеркальной защиты.
- | Для того чтобы выключить зеркальную защиту с помощью IBM Systems Director Navigator for i5/OS, выполните следующие действия:
 - | 1. Выберите **Настройка и обслуживание** в окне IBM Systems Director Navigator for i5/OS.
 - | 2. Выберите **Пулы дисков**.
 - | 3. Выберите пул дисков для выключения зеркальной защиты.
 - | 4. В меню **Выбрать действие** выберите **Выключить зеркальную защиту**.

- | Для того чтобы выключить зеркальную защиту с помощью System i Navigator, выполните следующие действия:
 - | 1. В окне System i Navigator разверните запись **Мои соединения** (или активную среду).
 - | 2. Разверните систему System i и выберите **Настройка и обслуживание** → **Аппаратное обеспечение** → **Диски** → **Пулы дисков**.
 - | 3. Выберите диск для выключения зеркальной защиты.
 - | 4. Щелкните на выбранном диске правой кнопкой мыши и выберите **Выключить зеркальную защиту**.
 - | 5. В открывшемся окне диалога выберите **Выключить зеркальную защиту**.

Добавление накопителя или дискового пула

- | Мастер Добавить диск позволяет добавить новый или ненастроенный дисковый накопитель в существующий пул дисков.
- | Мастеры Добавить диск и Добавить пул дисков объединяют несколько долго выполняемых функций конфигурации в один эффективный процесс. Кроме того, благодаря предварительному анализу возможностей системы, они предлагают только допустимые варианты, исключая тем самым выбор значений параметров дисков наугад. Например, система не поддерживает сжатие данных, то соответствующая опция будет недоступна в мастере.
- | При добавлении дисков в защищенный пул дисков мастер требует их добавления в набор устройств с проверкой четности или добавления достаточного числа дисков одинаковой емкости для запуска зеркальной защиты. Кроме того, в мастере доступны опции распределения и сжатия данных в пуле дисков, если это разрешено в конфигурации системы. Выберите нужные опции для настройки решения с учетом особенностей системы.
- | Для добавления диска или пула дисков с помощью IBM Systems Director Navigator for i5/OS выполните следующие действия:
 - | 1. Выберите **Настройка и обслуживание** в окне IBM Systems Director Navigator for i5/OS.
 - | 2. Выберите **Диски**.
 - | 3. В меню **Выбрать действия** выберите **Добавить диск**.
 - | 4. Добавьте диски в пул дисков в соответствии с инструкциями мастера.

- | Для добавления диска или пула дисков с помощью System i Navigator выполните следующие действия:
- | 1. В окне System i Navigator разверните запись **Мои соединения** (или активную среду).
- | 2. Разверните систему System i и выберите **Настройка и обслуживание** → **Аппаратное обеспечение** → **Диски**.
- | 3. Для добавления дисков щелкните правой кнопкой мыши на записи **Все диски** и выберите **Добавить диск**.
- | 4. Завершите выполнение задачи, следуя инструкциям мастера.

Оценка текущей конфигурации

Перед внесением изменений в конфигурацию дисков системы важно определить точное расположение существующих дисковых накопителей по отношению к пулам дисков, адаптерам ввода-вывода и стойкам.

В программе System i Navigator отображается графическое представление текущей конфигурации системы, что позволяет отказаться от сбора этой информации вручную. С помощью графического интерфейса можно выполнить все действия, доступные в списке Дисковые накопители System i Navigator, работая при этом с графическим представлением. В контекстном меню любого объекта в таблице (например, дискового накопителя, пула дисков, набора устройств с проверкой четности или стойки) доступен тот же набор опций, что и в главном окне System i Navigator.

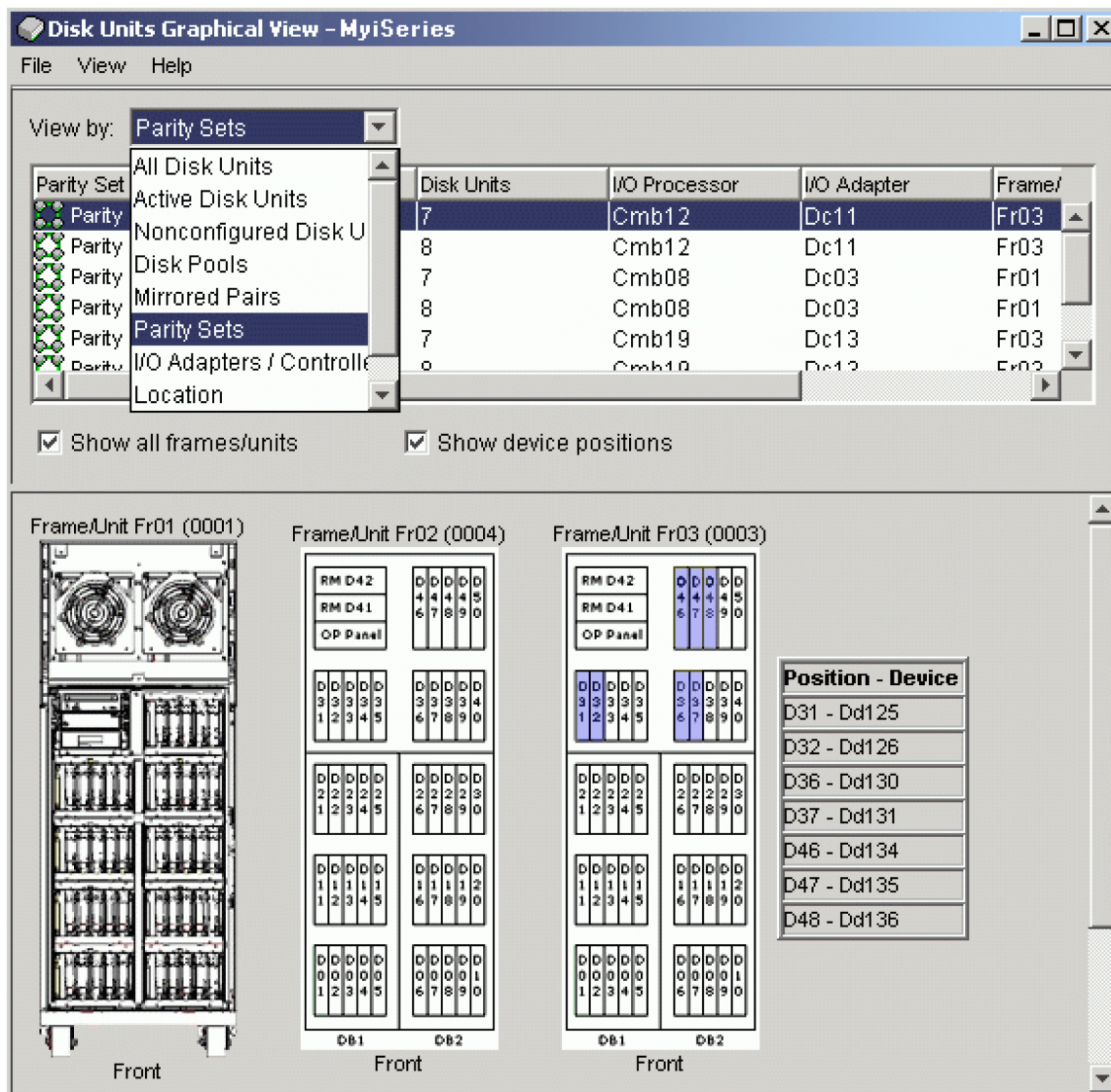
В окне Графическое представление дисковых накопителей можно выбрать способ отображения аппаратного обеспечения. Например, в списке пулов дисков можно выбрать конкретный пул дисков для отображения расположенных в нем стоек с дисками. Опция Показать все стойки позволяет просмотреть все стойки выбранного пула дисков вне зависимости от того, установлены ли в них дисковые накопители. Кроме того, можно выбрать опцию Показать все расположения устройств, для того чтобы связать имена дисков с расположениями, в которых они установлены.

На диске, выделенном синем цветом, можно щелкнуть правой кнопкой мыши и выбрать действие. Например, можно запустить или остановить сжатие данных на диске, добавить и удалить диск из набора устройств с проверкой четности или переименовать диск. Можно приостановить и возобновить зеркальную защиту диска. Щелкнув правой кнопкой мыши на пустом отсеке, вы можете запустить мастер Установить диск.

Для активации графического представления выполните следующие действия:

- 1. В окне System i Navigator разверните запись **Мои соединения** (или активную среду).
- 2. Разверните систему System i и выберите **Настройка и обслуживание** → **Аппаратное обеспечение** → **Диски**.
- 3. Щелкните правой кнопкой на записи **Все диски** и выберите **Графическое представление**.

Ниже приведен пример графического представления в System i Navigator. Меню Просмотр по позволяет просмотреть несколько опций для просмотра дисков.



Настройка доступа к пулу дисков

Для обращения к дисковым накопителям в независимом пуле дисков необходимо сделать пул дисков доступным (включить его).

Для обращения к дисковым накопителям в независимом пуле дисков и объектам связанной базы данных пул дисков необходимо сделать доступным (включить его). В случае применения географической зеркальной защиты требуется настроить доступ к рабочей копии пула дисков. Доступ к зеркальной копии можно настроить только после выключения на ней функции зеркальной защиты. Перед включением пула дисков с географической зеркальной защитой необходимо запустить группу переносимых устройств (если географическая зеркальная защита не выключена).

В среде кластера пул дисков можно сделать доступным на текущем или другом узле кластера. Независимый пул дисков одновременно можно включить только на одном узле. Для обращения к независимому пулу дисков из другого узла необходимо переключить независимый пул дисков на резервный узел кластера. Дополнительная информация о переносе CRG (в System i Navigator - группа переносимых устройств) на резервный узел приведена в разделе Выполнение переноса ресурсов.

Примечание: Вместе с основным или дополнительным пулом дисков доступными становятся все пулы дисков из группы пулов дисков.

В ходе включения пула дисков или настройки дисков из независимого пула дисков вам может показаться, что обработка остановилась. Операции операции включения пула дисков и настройки дисков ждут завершения других операций по настройке устройств.

Ошибки на ранних этапах включения пула дисков с географической зеркальной защитой могут привести к полной синхронизации в ходе следующей операции включения или возобновления.

Для того чтобы сделать независимый пул дисков доступным, выполните следующие действия:

1. В окне System i Navigator разверните запись **Мои соединения** (или активную среду).
2. Разверните систему System i и выберите **Настройка и обслуживание** → **Аппаратное обеспечение** → **Диски**.
3. Выберите **Пулы дисков**.
4. Щелкните правой кнопкой мыши на недоступном пуле дисков и выберите **Сделать доступным**.
Одновременно можно включить несколько выбранных пулов дисков.
5. В открывшемся окне выберите **Сделать доступным** для включения пула дисков.

Пул дисков можно сделать доступным из командной строки с помощью команды Изменить состояние конфигурации (VFYCFG).

Команда Показать состояние ASP (DSPASPSTS) позволяет определить обрабатываемый пул дисков.

Настройка распределенной по сайтам зеркальной защиты

Распределенная по сайтам зеркальная защита - это собирательный термин, используемый для обозначения нескольких различных технологий высокой готовности, включая географическую зеркальную защиту, синхронное зеркальное копирование и глобальное зеркальное копирование. У каждой из этих технологий есть определенные задачи по настройке.

Настройка географической зеркальной защиты

Географическая зеркальная защита - это подфункция распределенной по сайтам зеркальной защиты. Для настройки решения высокой готовности с помощью географической зеркальной защиты необходимо настроить сеанс зеркальной защиты между рабочей и резервной системами.

Прежде чем настраивать географическую зеркальную защиту, необходимо, чтобы имелись активный кластер, узлы и группа ресурсов кластера. Также для завершения настройки независимые ASP, которые будут использоваться для географической зеркальной защиты, должны быть выключены. В разделе Сценарий: Распределенная по сайтам зеркальная защита с географической зеркальной защитой приведены пошаговые инструкции по настройке решения высокой готовности на основе географической зеркальной защиты.

Навигатор IBM Systems Director для i5/OS

Для настройки географической зеркальной защиты с помощью Навигатора IBM Systems Director для i5/OS выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите **Настройка и службы** в окне Навигатора IBM Systems Director для i5/OS.
4. Выберите **Пулы дисков**.
5. Выберите пул дисков, который должен применяться как рабочая (исходная) копия.
6. В меню **Выбор действий** выберите **Создать сеанс**.
7. Для завершения задачи следуйте инструкциям мастера.

Навигатор System i

Для настройки географической зеркальной защиты с помощью Навигатора System i выполните следующие действия:

1. В Навигаторе System i разверните **Соединения** (либо активную среду).
2. Разверните систему, которую необходимо использовать в качестве рабочей копии.
3. Разверните **Настройка и службы** → **Аппаратное обеспечение** → **Дисковые накопители** → **Пулы дисков**.
4. Щелкните правой кнопкой мыши на пуле дисков, который необходимо использовать в качестве рабочей копии, и выберите **Сеансы** → **Создать**.
5. Для завершения задачи следуйте инструкциям мастера.

Понятия, связанные с данным

“Сценарий: Коммутируемый диск с географической зеркальной защитой” на стр. 78

В данном сценарии описано решение высокой готовности i5/OS, использующее коммутируемые диски с географической зеркальной защитой в кластере с тремя узлами. Данное решение обеспечивает как восстановление после аварии, так и высокую готовность.

Настройка сеанса синхронного зеркального копирования

Для решений высокой готовности i5/OS, использующих технологию синхронного зеркального копирования IBM System Storage, необходимо настроить сеанс между компьютером System i и внешними блоками памяти IBM System Storage, на которых настроено синхронное зеркальное копирование. В i5/OS сеансы синхронного зеркального копирования не отвечают за настройку зеркального копирования на внешних блоках памяти, а скорее устанавливают связь между системами i5/OS и существующей конфигурацией синхронного зеркального копирования на внешних блоках памяти.

Прежде чем создать сеанс синхронного зеркального копирования в i5/OS, необходимо настроить синхронное зеркальное копирование на внешних блоках памяти IBM System Storage. Со сведениями об использовании синхронного зеркального копирования на IBM System Storage DS6000 можно ознакомиться в IBM System Storage DS6000 Information Center. Со сведениями об использовании синхронного зеркального копирования на IBM System Storage DS8000, можно ознакомиться в IBM System Storage DS8000 Information Center.

Для настройки сеанса синхронного зеркального копирования выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите **Настройка и службы** в окне Навигатора IBM Systems Director для i5/OS.
4. Выберите **Пулы дисков**.
5. Выберите пул дисков, который должен применяться как рабочая (исходная) копия.
6. В меню **Выбор действий** выберите **Создать сеанс**.
7. Для завершения задачи следуйте инструкциям мастера.

Информация, связанная с данной

Команда Добавить описание копии ASP (ADDASPCPYD)

Команда Запустить сеанс ASP (STRASPSSN)

Настройка сеанса глобального зеркального копирования

Для решений высокой готовности i5/OS, использующих технологию глобального зеркального копирования IBM System Storage, необходимо настроить сеанс между компьютером System i и внешними блоками памяти IBM System Storage, на которых настроено глобальное зеркальное копирование. В i5/OS сеансы глобального зеркального копирования не отвечают за настройку зеркального копирования на внешних блоках памяти, а скорее устанавливают связь между системами i5/OS и существующей конфигурацией глобального зеркального копирования на внешних блоках памяти.

Технология глобального зеркального копирования IBM System Storage рассчитана на совместное использование всеми пользователями одного соединения для глобального зеркального копирования. Для применения глобального зеркального копирования высокой готовности в i5/OS на определенном сервере System Storage глобальное зеркальное копирование может быть настроено только в одном разделе System i.

Никакие другие разделы System i или серверы из других платформ не могут использовать глобальное зеркальное копирование в тот же момент. Добавление более одного пользователя к сеансу глобального зеркального копирования может вызвать непредсказуемый результат.

Прежде чем создать сеанс глобального зеркального копирования в i5/OS, необходимо настроить глобальное зеркальное копирование на внешних блоках памяти IBM System Storage. Со сведениями об использовании глобального зеркального копирования на IBM System Storage DS6000 можно ознакомиться в IBM System Storage DS6000 Information Center. Со сведениями об использовании глобального зеркального копирования на IBM System Storage DS8000, можно ознакомиться в IBM System Storage DS8000 Information Center.

Для настройки глобального зеркального копирования выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите **Настройка и службы** в окне Навигатора IBM Systems Director для i5/OS.
4. Выберите **Пулы дисков**.
5. Выберите пул дисков, который должен применяться как рабочая (исходная) копия.
6. В меню **Выбор действий** выберите **Создать сеанс**.
7. Для завершения задачи следуйте инструкциям мастера.

Информация, связанная с данной

Команда Добавить описание копии ASP (ADDASPCPYD)

Команда Запустить сеанс ASP (STRASPSSN)

Управление решением высокой готовности

После настройки решения высокой готовности i5/OS можно приступить к управлению этим решением с помощью интерфейсов, связанных с обеспечением высокой готовности.

Сценарии: Управление решениями высокой готовности

Системный оператор или администратор решения высокой готовности отвечает за выполнение таких задач общего характера, как резервное копирование и обслуживание системы в среде высокой готовности.

В следующих сценариях описаны инструкции по выполнению типичных задач, таких как резервное копирование и обновление, а также приведены примеры работы с событиями в среде высокой готовности, например, обслуживание разделов кластера или восстановление после сбоя. Каждый сценарий применяется в модельной среде. Инструкции сценариев соответствуют описанным решениям высокой готовности и могут использоваться только в качестве примеров.

Сценарии: Выполнение резервного копирования в среде высокой готовности

В зависимости от решения высокой готовности и стратегии резервного копирования могут применяться различные методы резервного копирования. Однако, существует общий набор задач при выполнении операций резервного копирования для систем в среде высокой готовности.

В некоторых решениях высокой готовности имеется возможность выполнения удаленного резервного копирования со второй копии данных, хранимой в резервной системе. Удаленное резервирование позволяет не прерывать функционирование рабочей системы в то время, как производится резервное копирование второй системы. Каждый сценарий содержит примеры двух решений высокой готовности, в которых резервное копирование осуществляется удаленно с помощью резервной системы.

В первом сценарии удаленное резервное копирование осуществляется в решении высокой готовности, использующем технологию географической зеркальной защиты. Во втором сценарии показано, как FlashCopy можно использовать в среде высокой готовности, где применяются решения IBM System Storage, как, например, синхронное или глобальное зеркальное копирование.

Сценарий: Резервное копирование в среде с географической зеркальной защитой:

В сценарии дано общее представление о задачах, которые необходимо выполнить при удаленном резервном копировании решения высокой готовности i5/OS, которое использует географическую зеркальную защиту.

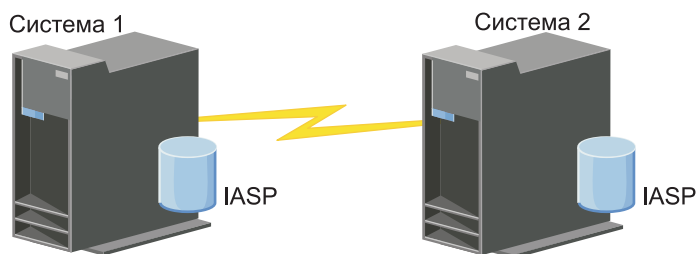
Обзор

В примере описана ситуация, в которой системному администратору требуется создать резервную копию данных, которые хранятся на независимых пулах дисков, используемых решением высокой готовности, основанном на технологии географической зеркальной защиты. Администратор не желает влиять на производительность системы, переводя ее в автономный режим. Вместо этого он намерен временно отсоединить зеркальную копию, а затем выполнить резервное копирование из второй копии данных, находящейся на независимых пулах дисков в удаленном расположении.

Примечание: При отключении зеркальной копии работа географической зеркальной защиты будет приостановлена до момента, когда она будет подключена снова. Пока она остается отсоединенной, высокая готовность и восстановление после аварии недоступны. Если во время этого процесса случится простой системы, то некоторые данные будут потеряны.

Дополнительные сведения

Эта среда изображена на следующем рисунке:



Этапы настройки

1. Выполнение приостановки независимого пула дисков
2. “Отсоединение зеркальной копии” на стр. 154
3. Добавление пула в число используемых
4. Резервное копирование независимого пула дисков
5. “Возобновление работы независимого пула дисков” на стр. 152
6. “Присоединение зеркальной копии” на стр. 155

Сценарий: Выполнение FlashCopy:

В данном примере администратору необходимо выполнить резервное копирование удаленной копии данных, хранящихся на внешних устройствах, выступающих в роли резервной системы. С помощью функции FlashCopy, доступной среди Устройств внешней памяти IBM, администратор может значительно сократить время резервного копирования.

Обзор

В данном примере системному администратору необходимо выполнить резервное копирование данных, хранящихся на внешних блоках системной памяти IBM System Storage. Администратор не хочет переводить рабочую систему в автономный режим для выполнения резервного копирования. Вместо этого он планирует выполнить FlashCopy, в результате чего будет осуществлен синхронный сбор данных. С этих данных и будет

снята резервная копия, сохраняемая на внешний диск. FlashCopy занимает всего несколько секунд и, таким образом, сокращает время всего процесса резервного копирования.

Хотя в данном примере FlashCopy применяется для операций резервного копирования, нужно отметить, что FlashCopy имеет несколько предназначений. Например, FlashCopy можно использовать для долговременного хранения данных, чтобы уменьшить нагрузку по запросам на рабочие системы, или для копирования рабочих данных при создании среды тестирования.

Шаги настройки

1. “Выполнение приостановки независимого пула дисков” на стр. 152
2. “Настройка сеанса FlashCopy” на стр. 160
3. Выполнение FlashCopy для внешних блоков системной памяти IBM System Storage. Со сведениями об использовании FlashCopy для IBM System Storage DS6000 можно ознакомиться в IBM System Storage DS6000 Information Center. Со сведениями об использовании FlashCopy для IBM System Storage DS8000, можно ознакомиться в IBM System Storage DS8000 Information Center.
4. “Возобновление работы независимого пула дисков” на стр. 152
5. Добавить ASP в число используемых
6. Резервное копирование независимого ASP

Сценарий: Обновление операционной системы в среде высокой готовности

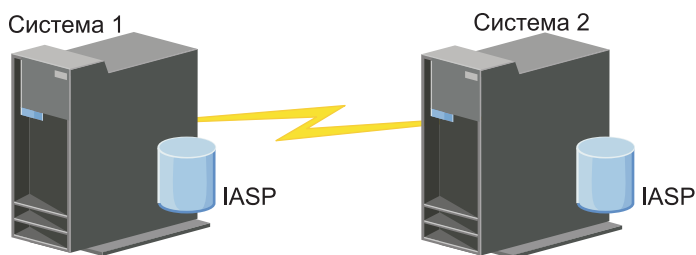
В этом примере системный администратор обновляет операционную систему в двух системах i5/OS в решении высокой готовности на базе географической зеркальной защиты.

Обзор

Системному администратору требуется обновить операционную систему в двух системах в среде высокой готовности. В данном примере два активных узла: System 1 и System 2. System 1 - рабочая копия, System 2 - зеркальная копия. В обеих системах работает ОС i5/OS V5R4. Независимый пул дисков включен, географическая зеркальная защита активирована, системы синхронизированы. Системному администратору необходимо обновить обе систем до i5/OSV6R1.

Описание

На приведенном ниже рисунке представлена данная среда:



Этапы настройки

1. Отсоедините зеркальную копию (System 2).
2. Завершите работу CRG (System 2).
3. Остановите узел (System 2).
4. Установите новый выпуск ОС в System 2. Дополнительная информация приведена в разделе Обновление или замена i5/OS и связанного ПО.
5. Установите лицензионную программу IBM System i High Availability Solutions Manager (iHASM) (5761-HAS).

6. Сделайте пул дисков доступным и протестируйте приложения в System 2. Тестирование приложений позволяет убедиться, что они работают должным образом в новом выпуске ОС. После завершения тестирования приложений можно выполнить остальные действия.
7. Сделайте пул дисков недоступным в отсоединенной зеркальной копии (System 2).
8. Присоедините зеркальную копию. Таким образом будет инициирована синхронизация копий данных. После выполнения синхронизации можно продолжить процедуру обновления.
9. “Перенос ресурсов” на стр. 94. Зеркальная копия (System 2) таким образом становится новой рабочей копией, а рабочая копия (System 1) - новой зеркальной копией.

Примечание: Географическая зеркальная защита приостанавливается, поскольку нельзя выполнять географическое зеркальное копирование из V6R1 в V5R4. Можно без проблем выполнять географическое зеркальное копирование из V5R4 в V6R1. В этом сценарии географическая зеркальная защита приостанавливается после выполнения принудительного переноса ресурсов. На протяжении оставшейся части процедуры обновления данные не защищены, поскольку отсутствует подходящая резервная система.

10. Завершите работу CRG (System 1).
11. Остановите узел (System 1).
12. Установите новый выпуск ОС в System 1. Дополнительная информация приведена в разделе Обновление или замена i5/OS и связанного ПО.
13. Установите лицензионную программу IBM System i High Availability Solutions Manager (iHASM) (5761-HAS).
14. Запустите узлы (System 1).
15. Запустите CRG (System 1).
16. Возобновите зеркальное копирование.
17. Выполните принудительный перенос ресурсов. Таким образом, текущая зеркальная копия (System 1) снова станет рабочей, а текущая рабочая копия (System 2) - зеркальной. Это соответствует исходной конфигурации до обновления.

Пример: Обновление операционной системы:

В средах высокой готовности перед обновлением операционной системы требуется выполнить дополнительные действия.

Рассмотрите следующие примеры, для того чтобы определить конкретную процедуру обновления в среде кластера. Перед тем, как приступить к обновлению или выполнению предварительных действий, определите текущую версию кластера.

Пример 1: Обновляется узел i5/OS V5R4. На всех остальных узлах установлена операционная система i5/OS V5R4 или более поздних версий. Текущая версия кластера: 5.

Действие: Обновите узел до i5/OS V6R1. После обновления узла запустите на нем кластер.

Пример 2: Обновляется узел i5/OS V5R4. На всех остальных узлах установлена операционная система i5/OS V5R4. Текущая версия кластера: 4.

Действие: Измените текущую версию кластера до 5. Обновите узел до i5/OS V6R1. Запустите кластер на обновленном узле.

Пример 3: Обновляется узел i5/OS V5R3. На всех остальных узлах установлена операционная система i5/OS V5R4. Текущая версия кластера: 4.

Действие: Удалите узел, обновляемый до i5/OS V6R1, из кластера. Измените текущую версию кластера до 5. Обновите узел до i5/OS V6R1 и снова добавьте его в кластер.

Пример 4: Обновляется узел i5/OS V5R4. В состав кластера входят только узлы i5/OS V5R3 и i5/OS V5R4. Текущая версия кластера: 4. Обновление узла i5/OS V5R4 до i5/OS V6R1 менее важно по сравнению с обновлением узлов i5/OS V5R3.

Действия:

1. Удалите обновляемый узел из кластера.
2. Обновите узел до i5/OS V6R1.
3. Обновите оставшиеся узлы i5/OS V5R3 по крайней мере до i5/OS V5R4.
4. Укажите версию кластера 5.
5. Добавьте обновленный узел в кластер.

Сценарий 5: Обновляется узел i5/OS V5R4. В состав кластера входят только узлы i5/OS V5R3 и i5/OS V5R4. Текущая версия кластера: 4. Обновление узла i5/OS V5R4 до i5/OS V6R1 более важно по сравнению с обновлением узлов i5/OS V5R3.

Действия:

1. Удалите все узлы i5/OS из кластера.
2. Укажите версию кластера 5.
3. Обновите узел до i5/OS V6R1.
4. Запустите обновленный узел.
5. По мере обновления оставшихся узлов i5/OS V5R3 до i5/OS V5R4 их можно добавлять обратно в кластер.

Сценарий 6: Обновляется узел i5/OS V5R3. В состав кластера входит по крайней мере один узел i5/OS V5R3. Текущая версия кластера: 3 или более низкая.

Действие: Обновите все узлы до i5/OS V5R4. Измените версию кластера до 4. Обновите все узлы до i5/OS V6R1.

В следующей таблице приведены действия, выполняемые в ходе обновления среды кластера.

Таблица 7. Обновление узлов до i5/OS V6R1

Текущий выпуск обновляемого узла	Текущая версия кластера	Действия
V5R4	5	<ol style="list-style-type: none"> 1. Обновите узел до i5/OS V6R1. 2. Запустите обновленный узел.
V5R4	4	<ol style="list-style-type: none"> 1. Укажите версию кластера 5. 2. Обновите узел до i5/OS V6R1. 3. Запустите обновленный узел. <p>Примечание: Если на остальных узлах кластера установлен выпуск i5/OS V5R3, то за дополнительной информацией обратитесь к сценариям 4 и 5.</p>
V5R3	4 или более низкая	<p>Вариант А</p> <ol style="list-style-type: none"> 1. Удалите обновляемый узел из кластера. 2. Укажите версию кластера 5. 3. Обновите узел до V6R1. 4. Добавьте узел в кластер. <p>Вариант В</p> <ol style="list-style-type: none"> 1. Обновите все узлы до V5R4. 2. Укажите версию кластера 5. 3. Обновите все узлы до V6R1.

Сценарий: обеспечение высокой готовности устройств

Помимо независимого пула дисков, также можно обеспечить высокую готовность других поддерживаемых устройств. В данной ситуации администратору высокой готовности требуется обеспечить высокую готовность линий Ethernet.

Обзор

Системному администратору необходимо обеспечить высокую готовность линий Ethernet, используемых в решении высокой готовности. Текущая конфигурация обеспечивает высокую готовность во время плановых простоев с помощью двух систем с применением технологии переносимых дисков. В этом решении также используется домен управления кластером для управления и синхронизации изменений в рабочей среде решения высокой готовности. В этом примере предполагается, что и настройка высокой готовности, и настройка Ethernet успешно выполнены. Также предполагается, что текущее состояние высокой готовности - Активно, и все отслеживаемые ресурсы в среде согласованы. В этом примере описаны действия по настройке высокой готовности для линии Ethernet.

Этапы настройки

1. “Создание переносимых устройств” на стр. 126
2. “Добавление записей отслеживаемых ресурсов” на стр. 104
3. “Выбор атрибутов, которые необходимо отслеживать” на стр. 136

Управление кластерами

С помощью графического интерфейса службы ресурсов кластеров можно выполнять многие задачи, связанные с кластерной технологией, которая является основой решения высокой готовности i5/OS. Эти задачи помогают в управлении кластером и его обслуживании.

После настройки кластера в нем чаще всего выполняются следующие операции:

Операции над кластером

- Добавление узла в кластер
- Удаление узла из кластера
- Запуск узла кластера
- Завершение работы узла кластера
- Коррекция версии кластера
- Удалить кластер
- Изменение узла кластера

Операции над группами ресурсов кластера

- Создание новой CRG
- Удаление CRG
- Запуск CRG
- Добавление узла в группу ресурсов кластера
- Удаление узла из группы ресурсов кластера
- Завершение работы CRG
- Изменение домена восстановления для CRG
- Принудительный перенос ресурсов
- Добавление узла в домен устройств
- Удаление узла из домена устройств

Операции над доменом управления кластером

- Создание домена управления кластером
- Добавление отслеживаемых ресурсов
- Удаление домена управления кластером

Коррекция версии кластера

Версия кластера - это версия протокола связи, применяемого узлами кластера для обмена данными.

Понятие версии необходимо для обеспечения полной совместимости серверов кластера, поскольку на разных серверах могут быть установлены разные уровни программного обеспечения.

Для коррекции версии кластера нужно, чтобы новая (последняя, потенциальная) версия кластера была установлена на всех узлах. После коррекции версии кластера все узлы будут применять последнюю версию протокола связи. Номер версии можно увеличивать только на единицу. Номер версии кластера нельзя уменьшить. Если вам требуется уменьшить версию кластера, нужно удалить кластер и создать его вновь, задав нужную версию. Текущая версия кластера первоначально задается первым узлом кластера. Остальные узлы можно будет добавлять в кластер только в случае, если они поддерживают эту версию.

- | Если вы обновляете узел до нового выпуска, то необходимо убедиться в том, что узел имеет соответствующую версию кластера. Кластеры поддерживают разницу лишь в одну версию. Если все узлы кластера - одного выпуска, то перед сменой версии кластера необходимо обновить их до нового выпуска.
- | Это обеспечит возможность использования всех функций, связанных с новым выпуском. Подробные инструкции по обновлению до нового выпуска приведены в разделе “Сценарий: Обновление операционной системы в среде высокой готовности” на стр. 114.

Для проверки и замены версии кластера на узле выполните следующие инструкции.

- | 1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
- | 2. Войдите в систему, указав пользовательский профайл и пароль.
- | 3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
- | 4. На странице Службы ресурсов кластеров выберите задачу **Показать свойства кластера**.
- | 5. На странице Свойства кластера щелкните на вкладке **Общие**.
- | 6. Проверьте версию кластера или замените ее требуемым значением.

Понятия, связанные с данным

Версия кластера

Информация, связанная с данной

Команда Изменить версию кластера (CHGCLUVER)

API Исправить версию кластера (QcstAdjustClusterVersion)

Удаление кластера

При удалении кластера во всех активных узлах кластера прекращается работа службы ресурсов кластера, все узлы удаляются из кластера.

- | Перед удалением кластера необходимо сделать активным по крайней мере один узел. Если в кластере есть переносимые диски или другие переносимые устройства, то перед удалением кластера необходимо удалить все узлы из домена устройств. В противном случае не удастся добавить диски в другой кластер.

Для удаления кластера выполните следующие действия:

- | 1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
- | 2. Войдите в систему, указав пользовательский профайл и пароль.
- | 3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
- | 4. На странице **Службы ресурсов кластеров** нажмите кнопку **Удалить кластер**.

5. Появится окно диалога подтверждения **Удалить кластер**. Для удаления кластера выберите **Да**. После удаления кластера на странице **Службы ресурсов кластеров** будет показано задание **Создать кластер. Задачи, связанные с данной**

“Удаление узла из домена устройств” на стр. 124

Домен устройств - множество узлов кластера, совместно использующих ресурсы устройств.

Информация, связанная с данной

Команда Удалить кластер (DLTCLU)

API Удалить кластер (QcstDeleteCluster)

Отображение конфигурации кластера

- Можно отобразить подробный отчет со сведениями о конфигурации кластера. Отчет о конфигурации кластера содержит подробные сведения о кластере, списке узлов, конфигурации и параметрах тонкой настройки, а также о каждой группе ресурсов кластера.

Для отображения сведений о конфигурации кластера выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице **Служба ресурсов кластера** выберите задачу **Отобразить сведения о конфигурации task**. Появится страница Конфигурация кластера и свойства. Эту страницу можно сохранить в виде файла или распечатать.

Информация, связанная с данной

- Команда Показать информацию о кластере (DSPCLUINF)

Сохранение и восстановление конфигурации кластера

Несмотря на то, что кластеры обладают высокой устойчивостью, ни в коем случае не следует пренебрегать резервным копированием.

Если кластер используется, в частности, для упрощения резервного копирования (на время сохранения данных с одной из систем работает другая, и наоборот), то настоятельно рекомендуется включить в кластер не менее трех систем. В этом случае при выходе системы из строя всегда будет наготове резервная система, даже если третья система в этот момент занята резервным копированием.

Сохранение и восстановление CRG

Группы ресурсов кластера можно сохранять как во время работы кластера, так и тогда, когда кластер выключен. Установлены следующие ограничения:

- Если кластер включен, то нельзя восстанавливать CRG, которые не определены в кластере.
- Если узел не входит в кластер, на нем нельзя восстановить CRG.

Группу ресурсов кластера можно восстановить в случае, если кластер включен, группа ресурсов кластера не определена в кластере, узел входит в домен восстановления CRG и имя кластера, указанное в определении CRG, совпадает с именем текущего кластера. Кроме того, группу ресурсов кластера можно восстановить, если кластер настроен, но служба ресурсов кластера не запущена на данном узле, а узел при этом входит в домен восстановления CRG.

Подготовка к критическим ситуациям

Серьезные сбои могут привести к необходимости повторной настройки кластера. На случай возникновения такой ситуации рекомендуется сохранить информацию о конфигурации кластера и держать под рукой распечатку этой информации.

1. После каждого изменения конфигурации кластера сохраняйте ее с помощью команды Сохранить конфигурацию (SAVCFG) или Сохранить систему (SAVSYS). Инструкции по применению операций SAVCFG и SAVSYS приведены в разделе Сохранение информации о конфигурации.
2. После каждого изменения конфигурации кластера создавайте бумажную копию параметров конфигурации. Распечатать конфигурацию кластера можно с помощью команды Показать информацию о кластере (DSPCLUINF). Храните ее копию вместе с резервными записями. Серьезные сбои могут привести к необходимости повторной настройки всего кластера.

Информация, связанная с данной

Сохранение данных конфигурации

Команда Сохранить конфигурацию (SAVCFG)

Сохранить систему (SAVSYS), команда

Команда Показать информацию о кластере (DSPCLUINF)

| Мониторинг состояния кластера

| Графический интерфейс служб ресурсов кластера отслеживает состояние кластера и показывает предупреждение о нарушениях в работе узлов решения высокой готовности.

| Графический интерфейс служб ресурсов кластера показывает предупреждение HAI0001W на странице Узлы при нарушении согласованности работы в кластере. Это сообщение означает, что информация, полученная от данного узла, может не совпадать с информацией из других активных узлов в кластере. Узлы становятся несогласованными, если они перестают быть активными в кластере.

| Для получения согласованной информации можно запросить ее у активного узла кластера или запустить этот узел и повторить запрос.

| Для мониторинга состояния кластера выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице Узлы показывается сообщение HAI0001W, если узел несогласован: Локальный узел кластера не работает. Информация кластера может быть неверной, пока локальный узел не будет запущен.

Задачи, связанные с данной

“Запуск узлов” на стр. 95

Операция запуска узла кластера заключается в запуске кластера и службы ресурсов кластера на узле в среде высокой готовности i5/OS.

Информация, связанная с данной

Команда Показать информацию о кластере (DSPCLUINF)

Команда Показать информацию о CRG (DSPCRGINF)

API Показать информацию о кластере (QcstListClusterInfo)

API Показать информацию о домене устройств (QcstListDeviceDomainInfo)

API Загрузить информацию о службах ресурсов кластера (QcstRetrieveCRSInfo)

API Загрузить информацию о кластере (QcstRetrieveClusterInfo)

API Показать группы ресурсов кластера (QcstListClusterResourceGroups)

API Показать информацию о CRG (QcstListClusterResourceGroupInf)

| Задание очередей сообщений

| Можно задать либо очередь сообщений кластера, либо очередь сообщений переноса ресурсов. С помощью этих очередей сообщений можно будет определить причины сбоев в среде высокой готовности i5/OS.

Очередь сообщений кластера используется сообщениями на уровне кластера и выдает одно сообщение, управляющее всеми группами ресурсов кластера, переносящими ресурсы на определенный узел. Очередь сообщений переноса ресурсов используется сообщениями на уровне группы ресурсов кластера и выдает одно сообщение на каждую группу, переносящую ресурсы.

Задание очереди сообщений кластера

Примечание: Настроить кластер для использования очереди сообщений кластера также можно, задав очередь сообщений при выполнении мастера Создание кластера.

Для задания очереди сообщений кластера выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице службы ресурсов кластера нажмите кнопку **Показать свойства кластера**.
5. На странице Свойства кластера нажмите кнопку **Очередь сообщений кластера**.
6. Для создания очереди сообщений кластера укажите следующую информацию:
 - В поле **Имя** укажите имя очереди сообщений для получения сообщений, имеющих отношение к автоматическому переносу ресурсов на уровне кластера или узла. Для переноса ресурсов на уровне узла отправляется одно сообщение, управляющее переносом всех групп ресурсов кластера с помощью одного и того же главного узла. Если перенос ресурсов группы осуществляется отдельно, отправляется одно сообщение, управляющее переносом ресурсов данной группы. Сообщение отправляется новому главному узлу. Если значение данного поля задано, указанная очередь сообщений должна существовать во всех узлах кластера при их запуске. Очередь сообщений не может находиться в независимом ASP.
 - В поле **Библиотека** укажите имя библиотеки, содержащей очередь сообщений для получения сообщения о переносе ресурсов. Библиотека не может называться *CURLIB, QTEMP, *LIBL, *USRLIBL, *ALL или *ALLUSR.
 - В поле **Время ожидания переноса ресурсов** выберите **Не ждать** или **Неограниченное время ожидания**, или укажите число минут ожидания ответа на сообщение о переносе ресурсов в очереди сообщений кластера.
 - В поле **Действие по умолчанию при переносе ресурсов** укажите действие, предпринимаемое Службой ресурсов кластера, когда время ответа на сообщение о переносе ресурсов превысило значение времени ожидания при переносе ресурсов. В этом поле можно задать значение **Продолжать перенос ресурсов** или **Отменить перенос ресурсов**.

Задание очереди сообщений переноса ресурсов

Для задания очереди сообщений переноса ресурсов выполните следующие действия:

1. В Web-браузере введите `http://mysystem:2001`, где mysystem - это имя хоста системы.
2. Войдите в систему по своему профайлу пользователя и паролю.
3. Выберите **Служба ресурсов кластера** в окне Навигатор IBM Systems Director для i5/OS.
4. На странице Служба ресурсов кластера выберите **Работа с группами ресурсов кластера**, чтобы просмотреть список групп ресурсов кластера.
5. Из списка групп ресурсов кластера выберите группу, с которой необходимо работать.
6. На странице Служба ресурсов кластера щелкните на меню **Выбрать действие** и выберите **Свойства**.
7. На странице Общие сведения введите следующие значения для задания очереди сообщений переноса ресурсов:
 - В поле **Очередь сообщений переноса ресурсов** укажите имя очереди сообщений для получения сообщений при переносе ресурсов для данной группы ресурсов кластера. Если значение данного поля

задано, указанная очередь сообщений должна существовать во всех узлах кластера домена восстановления после завершения работы программы выхода. Очередь сообщений переноса ресурсов не может находиться в независимом ASP.

- В поле **Библиотека** укажите имя библиотеки, содержащей очередь сообщений для получения сообщения о переносе ресурсов. Библиотека не может называться *CURLIB, QTEMP или *LIBL.
- В поле **Время ожидания переноса ресурсов** укажите число минут ожидания ответа на сообщение о переносе ресурсов в очереди сообщений переноса ресурсов. Также можно указать действие, предпринимаемое Службой ресурсов кластера, когда время ответа на сообщение о переносе ресурсов превысило указанное время ожидания при переносе ресурсов.

Справочная таблица по удалению кластера

Для того чтобы обеспечить полное удаление кластера, необходимо последовательно удалить различные компоненты кластера.

Таблица 8. Справочная таблица по удалению независимых ASP для кластеров

Требования к независимому ASP	
—	При использовании коммутируемых пулов дисков необходимо перенести блок расширения в узел, являющийся владельцем SPCN, прежде чем удалять группу ресурсов кластера. Для перемещения CRG обратно в узел-владельца SPCN можно использовать API Инициировать перенос ресурсов (QcstInitiateSwitchOver) или команду Изменить главный узел CRG (CHGCRGPRI). Если пропустить данный шаг, вы не сможете пометить блок расширения как частный для данной системы.
—	Если требуется удалить часть группы независимого ASP или, например, последний независимый ASP в перемещаемом устройстве, то сначала необходимо завершить работу CRG. Для этого можно применить команду Завершить работу CRG (ENDCRG).
—	Если требуется удалить независимый ASP, входящий в кластер, то настоятельно рекомендуется сначала удалить CRG устройств. Дополнительная информация приведена в разделе “Удаление CRG” на стр. 126. Для этой же цели можно воспользоваться командой Удалить запись устройства CRG (RMVCRGDEVE).
—	После удаления объекта конфигурации независимого ASP из переносимого устройства кластера можно удалить независимый ASP .
—	Удалите описание устройства для независимого ASP. Для этого выполните следующие действия: 1. В командной строке введите WRKDEVD DEVD(*ASP) и нажмите Enter. 2. Прокрутите текст до нужного описания устройства независимого ASP. 3. Выберите опцию 4 (Удалить) рядом с именем описания устройства и нажмите Enter.

Таблица 9. Справочная таблица по удалению группы ресурсов кластера

Требования к группе ресурсов кластера	
—	Для удаления группы ресурсов кластера можно воспользоваться любым из следующих действий: 1. Если узел не входит в кластер, то введите в командной строке команду DLTCRG CRG(CRGNAME). CRGNAME - это имя удаляемой CRG. Нажмите Enter. 2. Если узел входит в кластер, то введите в командной строке команду DLTCRGCLU CLUSTER(CLUSTERNAME) CRG(CRGNAME). CLUSTERNAME - имя кластера. CRGNAME - это имя удаляемой CRG. Нажмите Enter.

Управление узлами

Системы и логические разделы, входящие в состав среды высокой готовности i5/OS, называются узлами. В этом разделе описаны задачи управления, относящиеся к узлам.

Отображение свойств узла:

Можно отобразить и управлять свойствами, связанными с узлами, настроенными как часть среды высокой готовности, с помощью графического интерфейса Служба ресурсов кластера.

Для отображения свойств узла выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице **Службы ресурсов кластера** выберите задачу **Работа с узлами кластера**, чтобы просмотреть список узлов кластера.
5. На вкладке **Узлы** щелкните на меню **Выбрать действие** и выберите **Свойства**. Нажмите кнопку **Выполнить**. Появится страница Свойства узла.
 - На странице Общие показаны имя узла и системный IP-адрес этого узла.
 - На странице Кластер показаны следующие сведения:
 - IP-адреса интерфейса кластера используются для связи с другими узлами кластера.
 - В потенциальной версии узла указаны версия и уровень изменений, на котором узлы кластера поддерживают активную связь друг с другом.
 - Показаны домены устройств, настроенные в выбранном кластере. Если выбрать домен устройств в списке, также будут показаны узлы, принадлежащие выбранному домену.

Завершение работы узлов:

Запуск и завершение работы узла кластера сводятся к запуску и завершению работы службы ресурсов кластера на узле.

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На вкладке **Узлы** выберите узел, работу которого требуется завершить.
5. Откройте меню **Выбрать действие** выберите опцию **Остановить**. В результате запуска службы ресурсов кластера состояние узла должно измениться на Остановлен.

Информация, связанная с данной

Команда Завершить работу узла кластера (ENDCLUNOD)

API Завершить работу узла кластера (QcstEndClusterNode)

Удаление узлов:

- | Иногда возникает необходимость удалить узел из кластера, если выполняется обновление этого узла или если узел более не участвует в среде высокой готовности i5/OS.

Для удаления узла из существующего кластера выполните следующие действия:

- | 1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
- | 2. Войдите в систему, указав пользовательский профайл и пароль.
- | 3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
- | 4. На странице **Службы ресурсов кластера** выберите задачу **Работа с узлами кластера**, чтобы просмотреть список узлов кластера.
- | 5. На вкладке **Узлы** в меню **Выберите действие** выберите пункт **Удалить**.
- | 6. В окне подтверждения нажмите кнопку **Да**.

Задачи, связанные с данной

“Удаление географической зеркальной защиты” на стр. 156

Если вы больше не хотите применять географическую зеркальную защиту для определенного пула дисков или группы пулов дисков вы можете выбрать опцию **Удалить географическую зеркальную защиту**. После удаления географической зеркальной защиты система перестает осуществлять географическую зеркальную защиту и удаляет зеркальную копию пулов дисков из узлов на сайте зеркального копирования.

Информация, связанная с данной

Команда Удалить запись узла кластера (RMVCLUNODE)

API Удалить запись узла кластера (QcstRemoveClusterNodeEntry)

Удаление узла из домена устройств:

Домен устройств - множество узлов кластера, совместно использующих ресурсы устройств.

Важное замечание:

К удалению узлов из домена устройств следует относиться с предельным вниманием. Если по ошибке из домена устройств будет удален узел, выполняющий функции главной точки доступа, то домен устройств останется без главной точки доступа. Это означает, что все устройства домена станут недоступны.

После того как узел будет удален из домена устройств, его нельзя будет добавить обратно, если в этом домене устройств есть хотя бы один узел кластера. Для того чтобы добавить узел обратно в домен устройств, нужно выполнить следующие операции:

1. Удалить независимые ASP, принадлежащие узлу.
2. Перезапустить систему, выполнив IPL узла.
3. Добавить узел в домен устройств.
4. Вновь создать ASP, удаленный на шаге 1.

Для удаления узла из домена устройств выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице **Службы ресурсов кластера** выберите задачу **Работа с узлами кластера**, чтобы просмотреть список узлов кластера.
5. На вкладке **Узлы** в меню **Выберите действие** выберите **Свойства**. Нажмите кнопку **Перейти**. Откроется таблица Свойства узла.
6. На вкладке **Кластер** удалите имя узла в поле **Домен устройства** и нажмите кнопку **ОК**.

Задачи, связанные с данной

“Удаление кластера” на стр. 118

При удалении кластера во всех активных узлах кластера прекращается работа службы ресурсов кластера, все узлы удаляются из кластера.

Информация, связанная с данной

Команда Удалить запись домена устройств (RMVDEVDMNE)

API Удалить запись домена устройств (QcstRemoveDeviceDomainEntry)

Управление группами ресурсов кластера (CRG)

Группы ресурсов кластера (CRG) отвечают за управление устойчивыми ресурсами среды высокой готовности i5/OS. Они представляют собой технологию кластеров, которая управляет переключением ресурсов в резервные системы в случае сбоя.

Отображение состояния CRG:

1. Можно отслеживать состояние групп ресурсов кластера (CRG) в своей среде высокой готовности. Для оценки изменений CRG или определения неполадок CRG можно использовать эти сообщения о состоянии.

Для отображения состояния CRG выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.

2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице Служба ресурсов кластера выберите **Работа с группами ресурсов кластера**, чтобы просмотреть список групп ресурсов кластера.
5. На странице Служба ресурсов кластера просмотрите текущее состояние CRG в столбце Состояние.

Ниже приведены возможные значения для CRG:

Таблица 10. Значения состояние для CRG

Возможные значения	Описание
Запущена	CRG в данный момент запущена.
Остановлена	CRG в данный момент остановлена.
Под вопросом	Сведения об этой CRG в решении высокой готовности могут быть неточными. Такое состояние встречается, когда была вызвана программа выхода CRG для выполнения действия Отменить и в ее работе произошел сбой.
Восстановлена	CRG была восстановлена в узле и не копировалась на другие узлы кластера. При запуске кластера на узле CRG будет синхронизирована с другими узлами, и ее состояние изменится на Неактивна.
Неактивна	Служба ресурсов кластера для CRG неактивна на узле. На узле мог произойти сбой, работа узла могла быть завершена, или задание CRG не выполняется на этом узле.
Удаляется	CRG находится в процессе удаления из кластера.
Изменяется	CRG находится в процессе изменения. После завершения изменений CRG возвращается к предыдущему состоянию.
Останавливается	CRG находится в процессе остановки.
Добавляется	CRG находится в процессе добавления в кластер.
Запускается	CRG находится в процессе запуска.
В процессе переноса ресурсов	CRG находится в процессе переноса ресурсов на другой узел.
Добавление узла	В кластер добавляется новый узел. После успешного добавления узла CRG возвращается к предыдущему состоянию.
Удаление узла	Из CRG удаляется узел. После успешного удаления узла CRG возвращается к предыдущему состоянию.
Изменение состояния узла	В данный момент состояние узла, отвечающего за CRG в домене восстановления, изменяется.

Остановка CRG:

Группы ресурсов кластера (CRG) управляют устойчивыми ресурсами в среде высокой готовности i5/OS. Это технология кластера, определяющая и управляющая переносом устойчивых ресурсов в резервные системы в случае сбоя.

Необходимость остановки CRG может возникнуть с целью завершения работы функции автоматического переноса ресурсов в среде высокой готовности. Например, вы выполняете IPL в одной из систем, определенных в CRG.

Для остановки CRG выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице Служба ресурсов кластера выберите **Работа с группами ресурсов кластера**, чтобы просмотреть список групп ресурсов кластера.
5. На странице Служба ресурсов кластера выберите CRG, которую необходимо остановить.
6. В меню **Выбрать действие** выберите **Остановить** и нажмите кнопку **Выполнить**.

Информация, связанная с данной

Команда Завершить работу CRG (ENDCRG)

API Завершить работу CRG (QcstEndClusterResourceGroup)

Удаление CRG:

Удалить группу ресурсов кластера можно с помощью графического интерфейса Службы ресурсов кластера.

Для удаления CRG выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице Служба ресурсов кластера выберите **Работа с группами ресурсов кластера**, чтобы просмотреть список групп ресурсов кластера.
5. На странице Служба ресурсов кластера выберите CRG, которую необходимо удалить.
6. В меню **Выбрать действие** выберите **Удалить** и нажмите кнопку **Выполнить**.
7. Выберите **Да** в окне Подтверждение удаления группы ресурсов кластера.

Информация, связанная с данной

Команда Удалить CRG из кластера (DLTCRGCLU)

API Удалить CRG из кластера (QcstDeleteClusterResourceGroup)

Создание переносимых устройств:

Помимо независимых пулов дисков, для высокой готовности поддерживается несколько других устройств. Частью решения высокой готовности могут являться такие устройства, как линии Ethernet, оптические накопители, сетевые серверы и так далее.

Группа ресурсов кластера устройств содержит список переносимых устройств. Каждое устройство в списке соответствует переносимому независимому пулу дисков или переносимому устройству другого типа, например, накопителям на магнитной ленте, описаниям линий, контроллерам или сетевым серверам. При сбое все устройства в списке автоматически переносятся на резервный узел. Также можно включать устройства во время принудительного или автоматического переноса ресурсов.

Для создания переносимого устройства выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице Служба ресурсов кластера выберите **Работа с группами ресурсов кластера**, чтобы просмотреть список групп ресурсов кластера.
5. На странице Группа ресурсов кластера щелкните на значке контекста напротив группы ресурсов кластера устройств, к которой следует добавить существующее переносимое устройство, и в контекстном меню выберите опцию **Добавить существующее устройство**.
6. В списке **Добавить переносимое устройство** нажмите кнопку **Добавить**.

- | 7. В окне Добавить переносимое устройство укажите тип объекта конфигурации и имя объекта для переносимого устройства. Нажмите кнопку **ОК**, чтобы добавить переносимое устройство в список. Например, при добавлении переносимой линии Ethernet выберите Линия Ethernet.
- | 8. В окне списка нажмите кнопку **ОК**, чтобы добавить новое устройство в группу ресурсов кластера устройств.

Изменение домена восстановления для CRG:

Домен восстановления управляет восстановлением подмножества узлов, определенных в группе ресурсов кластера (CRG).

| Для изменения домена восстановления для группы ресурсов кластера устройств, группы ресурсов кластера приложений или группы ресурсов кластера данных выполните следующие действия:

- | 1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
- | 2. Войдите в систему, указав пользовательский профиль и пароль.
- | 3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
- | 4. На странице Служба ресурсов кластера выберите **Работа с группами ресурсов кластера**, чтобы просмотреть список групп ресурсов кластера.
- | 5. На странице Группа ресурсов кластера выберите CRG, которую требуется изменить.
- | 6. В меню **Выбрать действие** выберите **Свойства** и щелкните на **Перейти**.
- | 7. Для изменения заданных значений, связанных с доменом восстановления, щелкните на странице Домен восстановления. На этой странице можно изменить роли узлов, расположенных в домене восстановления кластера, а также добавить или удалить узлы из домена восстановления. Для группы ресурсов кластера устройств вы можете изменить место расположения и IP-адреса портов данных узла домена восстановления.

Информация, связанная с данной

Команда Добавить запись узла CRG (ADDCRGNODE)

Команда Изменить CRG (CHGCRG)

Команда Удалить запись узла CRG (RMVCRGNODE)

API Добавить узел в домен восстановления (QcstAddNodeToRcvyDomain)

API Изменить CRG (QcstChangeClusterResourceGroup)

API Удалить узел из домена восстановления (QcstRemoveNodeFromRcvyDomain)

| *Создание имен сайтов и IP-адресов портов данных:*

| При использовании географической зеркальной защиты узлы, определенные в узле домена восстановления CRG устройств, должны иметь IP-адрес порта данных и имя сайта.

| Имя сайта связано с узлом домена восстановления для CRG устройств и применяется только для географической зеркальной защиты. При настройке среды географической зеркальной защиты для высокой готовности каждый узел различных сайтов должен быть связан с различным именем сайта.

| Для создания IP-адреса порта данных и имен сайтов для узлов домена восстановления выполните следующие действия:

- | 1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
- | 2. Войдите в систему, указав пользовательский профиль и пароль.
- | 3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
- | 4. На странице Служба ресурсов кластера выберите задачу **Работа с группами ресурсов кластера**, чтобы просмотреть список групп ресурсов кластера.
- | 5. На вкладке Служба ресурсов кластера щелкните на контекстном значке рядом с CRG устройств и выберите **Свойства**.

- | 6. На странице Домен восстановления выберите **Изменить**.
- | 7. Для того чтобы использовать существующий IP-адрес порта данных, выберите его из списка и нажмите кнопку **ОК**. Для того чтобы добавить новый IP-адрес порта данных нажмите **Добавить**. В окне Добавление IP-адреса порта данных введите IP-адрес.
- | 8. В окне Изменить можно указать Имя сайта.

Управление событиями, вызывающими перенос ресурсов

Обычно автоматический перенос ресурсов выполняется при выходе узла из строя, но этим список причин не ограничивается. Перенос ресурсов может быть вызван различными действиями системы и пользователей.

Например, повреждение отдельного ресурса в группе ресурсов кластера (CRG) приведет к автоматическому переносу CRG, но при этом прочие CRG кластера останутся без изменения.

- | В кластере возможны простои четырех типов. Если перенос ресурсов вызван не простоем узла, то для определения причины и подходящих ответных действий может потребоваться дополнительное расследование. В следующей таблице описаны все категории простоев и указаны связанные типы событий и действия по исправлению.

Категория 1: Простой узла, вызывающий перенос ресурсов

| В ходе переносе ресурсов на уровне узла выполняются следующие действия:

- | • В каждой группе ресурсов кластера главный узел переводится в состояние *Неактивен* и становится последним резервным узлом.
- | • Узел, который был первым резервным узлом, становится главным узлом.

| Порядок переноса ресурсов:

- | 1. Все CRG устройств
- | 2. Все CRG данных
- | 3. Все CRG приложений

| Примечания:

- | 1. Если при попытке переноса какого-либо CRG выяснится, что нет ни одного рабочего резервного узла, CRG будет переведен в состояние *под вопросом* без изменения домена восстановления CRG.
- | 2. Для всех ресурсов кластера, для которых прекратила работу служба ресурсов кластера, будет выполнен автоматический перенос.

| Таблица 11. Категория 1: Простой узла, вызывающий перенос ресурсов

Событие, вызывающее перенос ресурсов
Выполнение команды ENDTCP(*IMMED или *CNTRLД с ограничением по времени)
Выполнение команды ENDSYS (*IMMED или *CNTRLД)
Выполнение команды PWRDWN SYS(*IMMED или *CNTRLД)
Нажатие кнопки IPL в момент, когда в системе запущена служба ресурсов кластера.
Вызов команды или API завершения работы узла кластера на основном узле домена восстановления CRG.
Вызов команды или API удаления узла кластера на основном узле домена восстановления CRG.
Выключение раздела с задержкой или выбор опции 7.
Выполнение команды ENDSBS QSYSWRK(*IMMED или *CNTRLД).
Отмена задания QCSTCTL (*IMMED или *CNTRLД с ограничением по времени).
Отмена задания QCSTCRGM (*IMMED или *CNTRLД с ограничением по времени).

Категория 2: Простой узла, вызывающий распад кластера

В случае этих простоев выполняются следующие действия:

- Для неотвечающих узлов кластера устанавливается состояние Распад. Дополнительная информация о распаде приведена в разделе Распад кластера.
- Все узлы в разделе кластера, у которых главный узел оказался в другом разделе, завершат работу с соответствующими CRG.

Примечания:

1. Если главный узел CRG выйдет из строя, но служба ресурсов кластера ошибочно посчитает, что произошел распад кластера, то все данные и приложения, которые обслуживались этим узлом, станут недоступны, а автоматический перенос ресурсов не будет выполнен.
2. В такой ситуации нужно либо объявить узел сбойным, либо восстановить работоспособность узла и вновь запустить на нем службу ресурсов кластера. Дополнительная информация приведена в разделе Перевод разделившихся узлов в разряд сбойных.

Таблица 12. Категория 2: Простой узла, вызывающий распад кластера

Событие, вызывающее перенос ресурсов
Простой аппаратного обеспечения СЕС (например, CPU).
Машинный сбой программного обеспечения операционной системы.
Немедленное выключение НМС или выбор опции 8.
Перезапуск раздела НМС или выбор опции 3.
Прекращение подачи питания СЕС.

Категория 3: Сбой группы ресурсов кластера, вызывающий перенос ресурсов

В ходе переноса ресурсов, вызванного сбоем CRG, выполняются следующие действия:

- Если неисправна только одна группа ресурсов кластера, то перенос ресурсов выполняется на уровне отдельной группы ресурсов кластера, поскольку групп ресурсов кластера независимы друг от друга.
- В случае отмены заданий нескольких групп ресурсов кластера выполняется несогласованный между группами ресурсов кластера перенос ресурсов.
- Главный узел переводится в состояние Неактивен и становится последним резервным узлом.
- Узел, который был первым резервным узлом, становится главным узлом.
- Если активные резервные узлы отсутствуют, то для CRG устанавливается состояние Под вопросом и домен восстановления остается без изменений.

Таблица 13. Категория 3: Сбой группы ресурсов кластера, вызывающий перенос ресурсов

Событие, вызывающее перенос ресурсов
Аварийное завершение задания CRG вследствие программной ошибки.
Сбой программы выхода приложения CRG.

Категория 4: Сбой системы связи, вызывающий распад кластера

Эта категория аналогична категории 2. Выполняются следующие действия:

- Для неотвечающих узлов кластера устанавливается состояние Распад. Дополнительная информация о распаде приведена в разделе Распад кластера.

- Все узлы и службы ресурсов кластера на узлах продолжают работу, однако не все узлы могут взаимодействовать друг с другом.
 - Кластер распадается, однако главные узлы CRG продолжают выполнять свои функции.
- Для автоматического возобновления работы кластера следует устранить неполадку связи, в результате которой произошел распад.

Примечание: Перед переключением CRG на новый главный узел убедитесь, что старый главный узел не использует ресурсы и пометьте его как неисправный. Дополнительная информация приведена в разделе Перевод разделившихся узлов в разряд сбойных.

Таблица 14. Категория 4: Сбой системы связи, вызывающий распад кластера

Событие, вызывающее перенос ресурсов
Выход из строя сетевого адаптера, линии или маршрутизатора.
ENDTCPIFC влияет на все целевые IP-адреса контрольного сигнала для узла кластера.

Простои с активными группами ресурсов кластера

- Если группа ресурсов кластера активна и неисправен *не* главный узел, то в ходе переноса выполняется следующее действие:
 - Обновление состояния неисправного элемента домена восстановления CRG.
 - Если узел, на котором возник сбой, был резервным узлом, то он перемещается в конец списка резервных узлов.
- Если группа ресурсов кластера активна и элементом домена восстановления является главный узел, то система выполняет действия в зависимости от типа простоя.
 - Категория 1: Простой узла, вызывающий перенос ресурсов
 - Категория 2: Простой узла, вызывающий распад кластера
 - Категория 3: Сбой группы ресурсов кластера, вызывающий перенос ресурсов
 - Категория 4: Сбой системы связи, вызывающий распад кластера

Простои с неактивными группами ресурсов кластера

- В случае простоя, связанного с CRG, выполняются следующие действия:
- Состояние неисправного узла в домене восстановления группы ресурсов кластера изменяется на Неактивен или Распад.
 - Роли узлов и порядок резервных узлов не изменяются.
 - Порядок резервных узлов в списке для неактивной группы ресурсов кластера можно изменить с помощью команды Запустить CRG (STRCRG) или API Запустить CRG (QcstStartClusterResourceGroup).

Примечание: API Запустить CRG нельзя применять в случае, если главный узел CRG не работает. В такой ситуации один из узлов следует сначала сделать главным с помощью команды Изменить группу ресурсов кластера (CHGCRG) command или API Изменить группу ресурсов кластера (QcstChangeClusterResourceGroup), а затем снова вызвать API Запустить CRG.

Управление доменом управления кластером

После создания домена управления кластером и добавления записей об отслеживаемых ресурсах администратору кластера необходимо какое-то время понаблюдать за работой этого домена, чтобы убедиться, что ресурсы в нем остаются согласованными. С помощью графического интерфейса службы ресурсов кластера можно управлять доменом управления кластером и контролировать его работу.

Этот графический интерфейс позволяет просматривать MRE и общее состояние каждого ресурса. Выбрав MRE, можно просмотреть более подробную информацию. Она включает в себя глобальное значение каждого атрибута, связанного с MRE, а также указание на то, соответствует ли атрибут домену. Если общее

состояние противоречит состоянию отслеживаемого ресурса, то администратор должен принять необходимые меры для определения и устранения причины ситуации, а потом повторно синхронизировать ресурс.

Если несогласованность возникла вследствие сбоя обновления на одном или нескольких узлах, то определить причину сбоя можно по данным, хранящимся для MRE. В журнал сбойного узла заносится сообщение, содержащее запись MRE сбойного ресурса. На других узлах будут информационные сообщения, свидетельствующие о неполадке, и перечень узлов, на которых не выполнено обновление. Доступ к этим сообщениям осуществляется через графический интерфейс службы ресурсов кластера или путем вызова API. Получить информацию о контролируемом ресурсе (QfpadRtvMonitoredResourceInfo). Сообщения о сбоях также регистрируются в протоколе смежного задания CRG.

Как только причина несогласованности будет определена, ресурс можно синхронизировать снова. Это можно сделать либо путем обновления "виноватого" узла, либо путем перезапуска домена управления. Например, несогласованность MRE для пользовательского профайла может возникнуть при смене ИД пользователя для пользовательского профайла на узле домена управления, если указанный ИД пользователя уже назначен другому пользовательскому профайлу на одном из узлов. Если заменить это значение ИД пользователя таким значением, которое не используется другим пользовательским профайлом в домене управления, то изменение будет произведено доменом управления кластером на всех узлах, и общее состояние MRE пользовательского профайла станет согласованным. После этого для синхронизации MRE пользовательского профайла не требуются дополнительные действия.

В некоторых случаях для синхронизации несогласованных ресурсов требуется завершить работу CRG домена управления кластером и перезапустить его. Например, если изменить ИД пользователя для пользовательского профайла, с которым связана MRE, когда пользовательский профайл участвует в задании на одном из узлов кластера в домене управления, то глобальное значение этой MRE будет несогласованным по причине сбоя операции изменения на том узле, на котором пользовательский профайл был активен. Для исправления ситуации требуется дождаться завершения задания, а затем завершить работу домена управления кластером. Когда домен управления будет запущен снова, глобальное значение каждого несогласованного атрибута будет использовано для перевода ресурса в согласованное состояние.

Если ресурс был удален, переименован или перемещен на другой узел домена, то общим состоянием отслеживаемого ресурса всегда устанавливается состояние сбоя. В такой ситуации необходимо удалить запись MRE, поскольку домену управления кластером больше не удастся синхронизировать этот ресурс.

При восстановлении отслеживаемого ресурса в какой-либо системе, входящей в домен управления кластером, этот ресурс синхронизируется с глобальным значением, которое известно в домене управления кластером во время активного состояния смежной CRG, представляющей домен управления кластером.

Синхронизация системных объектов происходит при выполнении следующих команд: RSTLIB, RSTOBJ, RSTUSRPRF и RSTCFG. Кроме этого, команды RSTSYSINF и UPDSYSINF вызывают синхронизацию системных значений и сетевых атрибутов. Для синхронизации системных переменных окружения после выполнения команды RSTSYSINF или UPDSYSINF необходимо завершить работу смежной CRG, представляющей домен управления кластером, и перезапустить ее.

При необходимости в восстановлении прежнего состояния отслеживаемых ресурсов, удалите MRE, представляющую ресурс, состояние которого требуется восстановить. Затем, после восстановления его состояния, добавьте MRE для ресурса из системы, в которой произведена операция восстановления. Домен управления кластером синхронизирует отслеживаемый ресурс в домене с использованием значений из восстановленного ресурса.

Для наблюдения за доменом управления кластером выполните следующие действия:

- | 1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
- | 2. Войдите в систему, указав пользовательский профайл и пароль.

- | 3. На странице Службы ресурсов кластера щелкните на опции **Работа с доменами управления**, чтобы просмотреть список доменов управления кластером в данном кластере.
- | 4. На вкладке **Домен управления** выберите **Создать домен управления**.
- | 5. На странице Создать домен управления введите информацию о домене управления кластером.

Остановка административного домена кластера:

Административные домены кластера обеспечивают устойчивость ресурсов, входящих в состав решения высокой готовности i5/OS. Административный домен кластера может потребоваться остановить с целью временного прекращения синхронизации отслеживаемых ресурсов.

В результате остановки административный домен кластера переходит в неактивное состояние. Пока административный домен кластера недоступен, все отслеживаемые ресурсы считаются несогласованными, поскольку вносимые в них изменения не синхронизируются. Несмотря на то, что отслеживание ресурсов не прекращается, глобальное значение не изменяется и внесенные изменения не передаются на остальные узлы административного домена. Синхронизация изменений, которые были внесены в отслеживаемые ресурсы, пока административный домен кластера был недоступен, выполняется после перезапуска административного домена кластера.

Примечание: Административный домен кластера и связанная с ним программа выхода поставляются IBM. Их не следует изменять с помощью API QcstChangeClusterResourceGroup или команды CHGCRG; в противном случае возникнут непредвиденные результаты.

Для того чтобы остановить административный домен кластера, выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. На странице службы ресурсов кластера нажмите кнопку **Работа с доменами управления**, чтобы увидеть список доменов управления кластером данного кластера.
4. На странице Домены управления выберите домен управления кластером.
5. В меню **Выбрать действие** выберите **Остановить**.
6. Нажмите кнопку **Да** на панели подтверждения остановки административного домена.

Информация, связанная с данной

Команда Завершить работу административного домена кластера (ENDCAD)

Удаление домена управления кластером:

Удалить домен управления кластером можно с помощью интерфейса Службы ресурсов кластера. После удаления домена управления кластером прекращается синхронизация отслеживаемых ресурсов, определенных в домене управления кластером.

Для удаления домена управления кластером выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. На странице службы ресурсов кластера нажмите кнопку **Работа с доменами управления**, чтобы увидеть список доменов управления кластером данного кластера.
4. На странице Домены управления выберите домен управления кластером.
5. В меню **Выбрать действие** выберите **Удалить**.
6. Нажмите кнопку **Да** на странице Подтверждение удаления домена управления кластером.

Изменение свойств домена управления кластером:

Изменить свойства существующего домена управления кластером можно с помощью графического интерфейса Служба ресурсов кластера. Это свойства, управляющие синхронизацией записей отслеживаемых ресурсов, определенных в домене управления кластером.

Для изменения свойств домена управления кластером выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. На странице службы ресурсов кластера нажмите кнопку **Работа с доменами управления**, чтобы увидеть список доменов управления кластером данного кластера.
4. На странице Домены управления выберите домен управления кластером.
5. В меню **Выбрать действие** выберите **Свойства**.
6. На странице Свойства можно изменить следующие сведения о домене управления кластером:
 - В поле **Имя** введите имя домена управления кластером. Имя должно состоять не более чем из 10 символов.
 - В поле **Опция синхронизации** укажите действия по синхронизации, когда узел присоединяется к домену управления кластером. Это поле включено, только если кластер относится к версии 6 или выше. Возможны следующие значения:

Опция Последние изменения (по умолчанию)

Выберите данную опцию, если необходимо применить все изменения отслеживаемых ресурсов к домену управления кластером. При присоединении узла к активному домену управления кластером любые изменения, внесенные в отслеживаемые ресурсы на этом узле в то время, как он был неактивен, применяются к отслеживаемым ресурсам на других активных узлах домена, если только не было более недавних изменений ресурса в активном домене. Последнее изменение отслеживаемого ресурса применяется к ресурсу на всех активных узлах.

Опция Активный домен

Выберите эту опцию, если изменения отслеживаемых ресурсов допускаются только на активных узлах. Изменения отслеживаемых ресурсов с неактивных узлов не принимаются во внимание при присоединении узла к домену управления кластером. Опция Активный домен не применяется к областям памяти сервера (*NWSSTG) или сетевым конфигурациям сервера (*NWSCFG). Синхронизация данных ресурсов всегда основана на последних сделанных изменениях.

- В списке **Узлы домена управления** можно либо добавить узел к домену управления кластером, выбрав **Добавить**, либо удалить узел из домена, выбрав **Удалить**.

Управление записями отслеживаемых ресурсов:

Графический интерфейс служб ресурсов кластера позволяет управлять записями отслеживаемых ресурсов в административном домене кластера. Административный домен кластера обеспечивает согласованность изменений отслеживаемых ресурсов в каждом узле среды высокой готовности.

Работа с состоянием записи отслеживаемого ресурса:

Графический интерфейс служб ресурсов кластера позволяет просматривать сообщения о состоянии записей отслеживаемых ресурсов, определенных в административном домене кластера.

После добавления MRE в административный домен кластера ресурса отслеживаются во всех узлах административного домена. Таким образом достигается синхронизация атрибутов ресурсов во всех узлах административного домена. Механизм синхронизации зависит от ряда факторов:

- Состояние кластера
- Состояние административного домена кластера
- Состояние узла
- Конкретные операции с ресурсом

Для работы с состоянием записи отслеживаемого ресурса выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профиль и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице службы ресурсов кластера нажмите кнопку **Работа с доменами управления**, чтобы увидеть список доменов управления кластером данного кластера.
5. На странице Домены управления щелкните на значке напротив домена управления кластером и выберите **Работа с типами отслеживаемых ресурсов**.

Примечание: Действие **Работа с типами отслеживаемых ресурсов** доступно, только если узел, с которым вы хотите работать, принадлежит домену управления кластером. Появится список типов отслеживаемых ресурсов.

6. На странице Работа с типами отслеживаемых ресурсов щелкните на значке рядом с типом ресурса и выберите **Атрибуты**.
7. Откроется список Атрибуты записи отслеживаемого ресурса. В столбце Глобальное состояние будет показано текущее состояние этого атрибута в активном административном домене кластера.

Состояние отслеживаемого ресурса в кластере определяют следующие значения:

Глобальное значение

Значение отслеживаемого атрибута, которое ресурс должен иметь во всех узлах административного домена. Глобальное значение будет одинаковым во всех активных узлах, оно представляет последнее синхронизированное изменение в домене.

Глобальное состояние

Это состояние ресурсов в административном домене кластера, определяющее, полностью ли синхронизированы ресурсы. Ниже приведены возможные значения:

Согласованное

Значения всех атрибутов ресурса, отслеживаемых системой, совпадают для всех активных узлов домена управления кластером. Это состояние в обычной рабочей среде, когда кластер, административный домен кластера и все узлы активны и работают. В такой среде все изменения значения отслеживаемого ресурса передаются во все другие узлы административного домена кластера. Обработка осуществляется асинхронно по отношению к исходному изменению, но при этом все ресурсы будут приведены в согласованное состояние в административном домене. При этом глобальное состояние будет согласованным, изменения будут применяться успешно во всех узлах, и значение ресурса в каждом узле будет совпадать с глобальным значением для ресурса.

Несогласованное

Значения всех атрибутов ресурса, отслеживаемых системой, не совпадают для всех активных узлов домена управления кластером. В протокол записывается сообщение о причине несогласованного состояния. Например, если изменения отслеживаемого ресурса происходят в момент, когда административный домен кластера не активен, то состояние отслеживаемого ресурса будет несогласованным.

Ожидание

Значения отслеживаемых атрибутов находятся в процессе синхронизации по домену управления кластером.

Добавление

Запись ресурса добавлена в административный домен кластера, но еще не синхронизирована.

Не работает

Отслеживаемый ресурс находится в неизвестном состоянии, потому что административный домен кластера прекратил работу, и изменения ресурса более не обрабатываются. Когда административный домен кластера завершает работу, глобальное состояние всех согласованных MRE становится нерабочим.

Сбой Ресурс более не отслеживается в административном домене кластера, и MRE необходимо удалить. Некоторые действия с ресурсами не рекомендуется выполнять во время синхронизации ресурса административным доменом кластера. Если ресурс, соответствующий MRE, является системным объектом, то для его удаления, переименования или перемещения в другую библиотеку следует сначала удалить MRE. В случае удаления, перемещения или переименования ресурса глобальное состояние MRE становится несогласованным, и последующие изменения этого ресурса не передаются в домен управления кластером.

После восстановления отслеживаемого ресурса в узле в административном домене кластера значения отслеживаемого ресурса согласуются с глобальными значениями посредством синхронизации в административном домене кластера.

Удаление записей отслеживаемых ресурсов:

Записи отслеживаемых ресурсов (MRE) - это ресурсы, используемые в данный момент в среде высокой готовности, изменения которых отслеживаются с помощью домена управления кластером. Если больше нет необходимости отслеживать MRE, их можно удалить. Записи отслеживаемых ресурсов (MRE) можно удалить с помощью графического интерфейса Службы ресурсов кластера.

Для удаления записи отслеживаемых ресурсов выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профиль и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице службы ресурсов кластера нажмите кнопку **Работа с доменами управления**, чтобы увидеть список доменов управления кластером данного кластера.
5. На странице Домены управления щелкните на значке напротив домена управления кластером и выберите **Работа с типами отслеживаемых ресурсов**.

Примечание: Действие **Работа с типами отслеживаемых ресурсов** доступно, только если узел, с которым вы хотите работать, принадлежит домену управления кластером. Появится список типов отслеживаемых ресурсов.

6. В списке типов отслеживаемых ресурсов щелкните на значке напротив типа отслеживаемых ресурсов и выберите **Удалить записи отслеживаемых ресурсов**. Появится список объектов MRE.
7. Щелкните на контекстном значке напротив объекта MRE, который необходимо удалить, и выберите **Удалить запись отслеживаемых ресурсов**.
8. Нажмите кнопку **Да** в окне Подтверждение удаления объекта MRE. Запись отслеживаемого ресурса будет удалена из домена управления кластером.

Информация, связанная с данной

Команда Удалить MRE административного домена (RMVCADMRE)

API удалить запись отслеживаемого ресурса (QfpadRmvMonitoredResourceEntry)

Просмотр типов отслеживаемых ресурсов:

Типы отслеживаемых ресурсов - это системные объекты, такие как пользовательские профили и переменные среды, которые могут отслеживаться в административном домене кластера. В этом разделе описано, как можно просмотреть список отслеживаемых ресурсов, которые заданы в административном домене кластера.

Для просмотра списка типов отслеживаемых ресурсов выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профиль и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.

4. На странице службы ресурсов кластера нажмите кнопку **Работа с доменами управления**, чтобы увидеть список доменов управления кластером данного кластера.
5. На странице Домены управления щелкните на значке напротив домена управления кластером и выберите **Работа с типами отслеживаемых ресурсов**.

Примечание: Действие **Работа с типами отслеживаемых ресурсов** доступно, только если узел, с которым вы хотите работать, принадлежит домену управления кластером. Появится список типов отслеживаемых ресурсов.

6. Выполните требуемые действия с выбранными типами отслеживаемых ресурсов:
 - Работа с атрибутами отслеживаемых ресурсов
 - Добавление записи отслеживаемого ресурса

| *Просмотр записей отслеживаемых ресурсов:*

| Записи отслеживаемых ресурсов - это ресурсы, такие как пользовательские профайлы и переменные среды, которые определены в административном домене кластера. Графический интерфейс служб ресурсов кластера позволяет просматривать записи отслеживаемых ресурсов, определенные в административном домене кластера.

| Для просмотра записей отслеживаемых ресурсов выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице службы ресурсов кластера нажмите кнопку **Работа с доменами управления**, чтобы увидеть список доменов управления кластером данного кластера.
5. На странице Домены управления щелкните на значке напротив домена управления кластером и выберите **Работа с типами отслеживаемых ресурсов**.
6. В списке типов отслеживаемых ресурсов щелкните на значке рядом с типов ресурса и выберите **Работа с записями отслеживаемых ресурсов**.
7. В открывшемся списке можно работать с записями отслеживаемых ресурсов.

Выбор атрибутов, которые необходимо отслеживать:

После добавления записей отслеживаемых ресурсов можно выбрать атрибуты, связанные с тем ресурсом, который необходимо отслеживать с помощью домена управления кластером.

Для выбора необходимых атрибутов для записи отслеживаемого ресурса (MRE) выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице службы ресурсов кластера нажмите кнопку **Работа с доменами управления**, чтобы увидеть список доменов управления кластером данного кластера.
5. На странице Домены управления щелкните на значке напротив домена управления кластером и выберите **Работа с типами отслеживаемых ресурсов**.

Примечание: Действие **Работа с типами отслеживаемых ресурсов** доступно, только если узел, с которым вы хотите работать, принадлежит домену управления кластером. Появится список типов отслеживаемых ресурсов.

6. В списке типов отслеживаемых ресурсов щелкните на значке контекста напротив нужного типа и выберите **Работа с записями отслеживаемых ресурсов....** Появится список объектов MRE.
7. Щелкните на значке контекста напротив объекта MRE, например, пользовательского профайла или системного значения, и выберите **Работа с атрибутами.** Появится список атрибутов MRE.
8. В окне Список атрибутов MRE выберите атрибуты, которые необходимо отслеживать, и нажмите кнопку **Закрывать.** Например, если необходимо отслеживать изменения атрибута имени ресурса для описания линии Ethernet, в качестве атрибута следует выбрать имя ресурса.

Задачи, связанные с данной

“Добавление записей отслеживаемых ресурсов” на стр. 104

В домен управления кластером можно добавить записи отслеживаемых ресурсов. В них определены важные ресурсы для того, чтобы изменения вносимые в эти ресурсы действовали для всей среды высокой готовности.

Атрибуты, которые можно отслеживать:

В домен управления кластером можно добавить записи для различных типов отслеживаемых ресурсов. В этом разделе перечислены атрибуты, которые можно отслеживать для каждого типа ресурсов.

Типы ресурсов

- Классы (*CLS)
- | • Описания линий Ethernet (*ETHLIN)
- Описания устройств независимых ASP (*ASPDEV)
- Описание заданий (*JOBDD)
- Сетевые атрибуты (*NETA)
- | • Конфигурация сетевого сервера для обеспечения безопасности соединения (*NWSCFG)
- | • Конфигурация сетевого сервера для удаленных систем (*NWSCFG)
- | • Конфигурация сетевого сервера для служебных процессоров (*NWSCFG)
- | • Описания сетевых серверов для соединений iSCSI (*NWSD)
- | • Описания сетевых серверов для интегрированных сетевых серверов (*NWSD)
- | • Области памяти сетевых серверов (*NWSSTG)
- | • Описания устройств адаптеров хостов сетевых серверов (*NWSHDEV)
- | • Описание оптических устройств (*OPTDEV)
- | • Описания подсистем (*SBSD)
- Переменные среды системы (*ENVVAR)
- Системные значения (*SYSVAL)
- | • Описания накопителей на магнитной ленте (*TAPDEV)
- | • Описания линий Token-Ring (*TRNLIN)
- Атрибуты TCP/IP (*TCPA)
- Пользовательские профайлы (*USRPRF)

Таблица 15. Атрибуты, которые можно отслеживать для классов

Имя атрибута	Описание
CPUTIME	Максимальное время CPU
DFTWAIT	Время ожидания по умолчанию
MAXTHD	Максимальное число нитей
MAXTMPSTG	Максимальный объем временной памяти
RUNPTY	Приоритет выполнения
ТЕХТ	Описание

Таблица 15. Атрибуты, которые можно отслеживать для классов (продолжение)

Имя атрибута	Описание
TIMESLICE	Квант времени

Таблица 16. Атрибуты, которые можно отслеживать для описаний линий Ethernet

Имя атрибута	Описание
ASSOCPORT	Связанное имя ресурса порта
AUTOCRTCTL	Контроллер автоматического создания
AUTODLTCTL	Контроллер автоматического удаления
CMNRCYLMT	Лимиты восстановления
COSTBYTE	Относительная стоимость за бит для отправки и получения данных по линии
COSTCNN	Относительная стоимость подключения к линии
DUPLEX	Дуплекс
GENTSTFRM	Создание тестовых кадров
GRPADR	Групповой адрес
LINESPEED	Быстродействие линии
MAXFRAME	Максимальные размеры кадра
MAXCTL	Максимальное число контроллеров
MSGQ	Очередь сообщений
ONLINE	Включать при IPL
PRPDLY	Задержка распространения
RSRCNAME	Имя ресурса
SECURITY	Уровень безопасности физической линии
SSAP	Информационный список Source service access point (SSAP)
TEXT	Описание
USRDFN1	Первый пользовательский
USRDFN2	Второй пользовательский
USRDFN3	Третий пользовательский
VRYWAIT	Ожидание включения

Таблица 17. Атрибуты, которые можно отслеживать для описаний устройств независимых ASP

Имя атрибута	Описание
MSGQ	Очередь сообщений
RDB	Реляционная база данных
RSRCNAME	Имя ресурса
TEXT	Описание

Таблица 18. Атрибуты, которые можно отслеживать для описаний заданий

Имя атрибута	Описание
ACGCDE	Код учета ресурсов
ALWMLTTHD	Разрешить несколько нитей
DDMCNV	Диалог DDM

Таблица 18. Атрибуты, которые можно отслеживать для описаний заданий (продолжение)

Имя атрибута	Описание
DEVRCYACN	Действие по восстановлению устройства
ENDSEV	Код серьезности завершения
HOLD	Блокировать при помещении в очередь
INLASGRP	Начальная группа ASP
INQMSGRPY	Ответ на сообщение-вопрос
JOBMSGQFL	Действие при заполнении очереди сообщений задания
JOBMSGQMX	Максимальный размер очереди сообщений задания
JOBPTY	Приоритет заданий (в JOBQ)
JOBQ	Очередь заданий
LOG	Занесение сообщений в протокол
LOGCLPGM	Занесение команд программы CL в протокол
OUTPTY	Приоритет вывода (в OUTQ)
OUTQ	Очередь вывода
PRTDEV	Принтер
PRTTXT	Текст для печати
RQSDTA	Данные или команда запроса
RTGDTA	Данные маршрутизации
SPLFACN	Действие буферного файла
SWS	Переключатели заданий
SYNTAX	Синтаксическая проверка CL
TEXT	Описание
TSEPOOL	Смена пула по истечении кванта времени
USER	Пользователь

Таблица 19. Атрибуты, которые можно отслеживать для сетевых атрибутов

Имя атрибута	Описание
ALWADDCLU	Разрешить добавление в кластер
DDMACC	Обработка запросов DDM/DRDA
NWSDOMAIN	Домен сетевого сервера
PCSACC	Обработка запросов клиентов
Примечание: Каждый сетевой атрибут трактуется как отдельная запись отслеживаемого ресурса. Поэтому тип ресурса и имена атрибутов совпадают.	

Таблица 20. Атрибуты, которые можно отслеживать для конфигураций сетевых серверов для служебных процессоров

Имя атрибута	Описание
EID	Идентификатор корпуса
ENBUNICAST	Включить направленную пересылку
INZSP	Инициализировать служебный процессор
SPAUT	Права доступа к служебному процессору
SPCERTID	Идентификатор сертификата служебного процессора

Таблица 20. Атрибуты, которые можно отслеживать для конфигураций сетевых серверов для служебных процессоров (продолжение)

Имя атрибута	Описание
SPINTNETA	IP-адрес служебного процессора
SPNAME	Имя служебного процессора
TEXT	Описание

Таблица 21. Атрибуты, которые можно отслеживать для конфигураций сетевых серверов для удаленных систем

Имя атрибута	Описание
BOOTDEVID	Идентификатор загрузочного устройства
CHARAUT	Идентификация CHAR целевого устройства
DELIVERY	Режим доставки
DYNBOOTOPT	Опции динамической загрузки
INRCHARAUT	Идентификация CHAR инициатора
RMTIFC	Удаленные интерфейсы
RMTSYSID	Идентификатор удаленной системы
SPNWSCFG	Конфигурация сетевого сервера служебного процессора, которая используется для управления удаленным сервером
TEXT	Описание

Таблица 22. Атрибуты, которые можно отслеживать для конфигураций сетевых серверов для защиты соединений

Имя атрибута	Описание
IPSECRULE	Правила защиты IP
TEXT	Описание

Таблица 23. Атрибуты, которые можно отслеживать для описаний сетевых серверов для интегрированных сетевых серверов

Имя атрибута	Описание
CFGFILE	Файл конфигурации
CODEPAGE	Кодовая страница ASCII, представляющая набор символов, который должен применяться данным сетевым сервером
EVTLOG	Протокол событий
MSGQ	Очередь сообщений
NWSSTGL	Ссылки области памяти
PRPDMNUSR	Распространить пользователя домена
RSRCNAME	Имя ресурса
RSTDDEVRSC	Ресурсы устройства, доступ к которому запрещен
SHUTDTIMO	Тайм-аут отключения
SYNCTIME	Синхронизация даты и времени
TCPDMNNAME	Имя локального домена TCP/IP
TCPHOSTNAM	Имя хоста TCP/IP
TCPPORTCFG	Конфигурация порта TCP/IP

Таблица 23. Атрибуты, которые можно отслеживать для описаний сетевых серверов для интегрированных сетевых серверов (продолжение)

Имя атрибута	Описание
TCPNAMSVR	Система сервера имен TCP/IP
TEXT	Описание
VRYWAIT	Ожидание включения
WINDOWSNT	Описание сетевого сервера Windows

Таблица 24. Атрибуты, которые можно отслеживать для описаний сетевых серверов для соединений iSCSI

Имя атрибута	Описание
ACTTMR	Таймер активации
CFGFILE	Файл конфигурации
CMNMSGQ	Очередь сообщений связи
CODEPAGE	Кодовая страница ASCII, представляющая набор символов, который должен применяться данным сетевым сервером
DFTSECRULE	Правило защиты IP по умолчанию
DFTSTGPTH	Путь к хранилищу по умолчанию
EVTLOG	Протокол событий
MLTPTHGRP	Группа с альтернативными путями
MSGQ	Очередь сообщений
NWSCFG	Конфигурация сетевого сервера
NWSSTGL	Ссылки области памяти
PRPDMNUSR	Распространить пользователя домена
RMVMEDPTH	Путь к съемному носителю
RSRCNAME	Имя ресурса
RSTDDEVRSRC	Ресурсы устройства, доступ к которому запрещен
SHUTDTIMO	Тайм-аут отключения
STGPTH	Пути к хранилищам iSCSI сетевого сервера
SYNCTIME	Синхронизация даты и времени
TCPDMNNAME	Имя локального домена TCP/IP
TCPHOSTNAM	Имя хоста TCP/IP
TCPNAMSVR	Система сервера имен TCP/IP
TCPPORTCFG	Конфигурация порта TCP/IP
TEXT	Описание
VRTETHCTLP	Управляющий порт виртуального Ethernet
VRTETHPTH	Путь виртуального Ethernet
VRYWAIT	Ожидание включения

Таблица 25. Атрибуты, которые можно отслеживать для областей памяти сетевых серверов

Имя атрибута	Описание
SIZE	Размер
TEXT	Описание

Таблица 25. Атрибуты, которые можно отслеживать для областей памяти сетевых серверов (продолжение)

Имя атрибута	Описание
TOTALFILES	Общее число файлов

Таблица 26. Атрибуты, которые можно отслеживать для описаний адаптеров сетевых серверов

Имя атрибута	Описание
CMNRCYLMT	Лимиты восстановления
LCLIFC	Связанный локальный интерфейс
MSGQ	Очередь сообщений
ONLINE	Включать при IPL
RSRCNAME	Имя ресурса
TEXT	Описание

Таблица 27. Атрибуты, которые можно отслеживать для описаний оптических накопителей

Имя атрибута	Описание
MSGQ	Очередь сообщений
ONLINE	Включать при IPL
RSRCNAME	Имя ресурса
TEXT	Описание

Таблица 28. Атрибуты, которые можно отслеживать для описаний подсистем

Имя атрибута	Описание
AJE	Запись задания автозапуска
CMNE	Включать при IPL
JOBQE	Очередь заданий
MAXJOBS	Максимальное число заданий
PJE	Запись предварительного задания
RMTLOCNAME	Имя удаленного расположения
RTGE	Запись о выполнении
SGNDSPF	Окно входа в систему
SYSLIBLE	Библиотека подсистем
TEXT	Описание
WSNE	Запись имени рабочей станции
WSTE	Запись типа рабочей станции

Таблица 29. Атрибуты, которые можно отслеживать для переменных среды системы

Можно отслеживать любую переменную среды уровня *SYS. Имя атрибута и имя ресурса совпадают с именем переменной среды.
Примечание: Каждая переменная среды трактуется как отдельная запись отслеживаемого ресурса. Поэтому тип ресурса и имена атрибутов совпадают.

Таблица 30. Атрибуты, которые можно отслеживать для переменных системных значений

Имя атрибута	Описание
QACGLVL	Уровень учета ресурсов
QACTJOBITP	Разрешить прерывание заданий
QALWOBJRST	Запрещает пользователям восстанавливать в системе системные объекты и объекты, принимающие права доступа.
QALWUSRDMN	Разрешает объекты пользовательского домена
QASTLVL	Уровень поддержки
QATNPGM	Программа Attention
QAUDCTL	Управление контролем
QAUDENDACN	Действие при ошибке журнала контроля
QAUDFRCLVL	Число записей в журнале контроля перед их сохранением
QAUDLVL	Уровень контроля
QAUDLVL2	Расширение уровня контроля
QAUTOCFG	Автоматическая настройка устройств
QAUTORMT	Удаленные контроллеры и устройства
QAUTOVRT	Автоматическая настройка виртуальных устройств
QCCSID	Идентификатор набора символов
QCFGMSGQ	Очередь сообщений для линий, контроллеров и устройств
QCHRID	Набор графических символов и кодовая страница, используемые по умолчанию для просмотра и печати данных
QCHRIDCTL	Управляющий элемент символьного идентификатора для задания
QCMNRCYLMT	Автоматическое восстановление после ошибок связи
QCNTYID	Идентификатор страны или региона
QCRTAUT	Права доступа к новым объектам
QCRTOBJAUD	Контроль новых объектов
QCTLSBSD	Управляющая подсистема или библиотека
QCURSYM	Символ денежной единицы
QDATFMT	Формат даты
QDATSEP	Разделитель даты
QDBRCVYWT	Ожидание восстановления базы данных перед выполнением перезапуска
QDECFMT	Десятичный формат
QDEVNAMING	Соглашение об именах устройств
QDEVRCYACN	Действие по восстановлению устройства
QDSCJOBITV	Интервал тайм-аута для отсоединенных заданий
QDSPSGNINF	Контролирует окно информации о входе в систему
QENDJOB LMT	Максимальное время ожидания перед принудительным завершением задания
QFRCCVNRST	Преобразование при восстановлении
QHSTLOGSIZ	Размер файла протокола хронологии

Таблица 30. Атрибуты, которые можно отслеживать для переменных системных значений (продолжение)

Имя атрибута	Описание
QIGCCDEFNT	Имя кодированного шрифта
QIGCFNTSIZ	Размер в пунктах кодированного шрифта
QINACTITV	Тайм-аут для неактивного задания
QINACTMSGQ	Действие после интервала тайм-аута
QIPLTYPE	Тип перезапуска
QJOBMSGQFL	Действие при заполнении очереди сообщений задания
QJOBMSGQMX	Максимальный размер очереди сообщений задания
QJOBMSGQSZ	Начальный размер очереди сообщений задания в килобайтах (Кб)
QJOBMSGQTL	Максимальный размер очереди сообщений задания в килобайтах (в Кб)
QJOBSPLA	Начальный размер блока управления буфером для задания (в байтах)
QKBDDBUF	Буфер клавиатуры
QKBDTYPE	Набор символов языка клавиатуры
QLANGID	Идентификатор языка по умолчанию
QLIBLCKLVL	Заблокировать библиотеки в списке поиска библиотек пользовательского задания
QLMTDEVSSN	Ограничить сеансы одним устройством
QLMTSECOFR	Ограничить права доступа системного администратора к устройству
QLOCALE	Локаль
QLOGOUTPUT	Генерация вывода на принтер для протокола задания
QMAXACTLVL	Максимальный уровень активности системы
QMAXJOB	Максимальное число заданий, разрешенных в системе
QMAXSGNACN	Ответ системы при достижении порогового значения, заданного системным значением QMAXSIGN
QMAXSIGN	Максимальное допустимое число неудачных попыток входа в систему
QMAXSPLF	Максимальное число файлов вывода на принтер
QMLTTHDACN	Если функция в многопоточном задании не поддерживает нити
QPASTHRSVR	Доступные серверные задания удаленного входа в систему дисплейной станции
QPRBFTR	Фильтр протокола неполадок
QPRBHLDITV	Минимальная отсрочка
QPRTDEV	Принтер по умолчанию
QPRTKEYFMT	Формат печати по клавише Print
QPRTTXT	До 30 символов текста можно напечатать в нижней части списков и разделительных страниц
QPWDCHGBLK	Минимальное время между изменениями пароля
QPWDEXPITV	Срок действия пароля (в днях)

Таблица 30. Атрибуты, которые можно отслеживать для переменных системных значений (продолжение)

Имя атрибута	Описание
QPWDEXPWRN	Системный интервал предупреждения об истечении срока действия пароля
QPWDLMTACJ	Указывает, разрешено ли указывать цифры в соседних позициях пароля
QPWDLMTCHR	Указывает, можно ли использовать определенные символы в пароле
QPWDLMTREP	Указывает, может ли пароль содержать повторяющиеся символы
QPWDLVL	Уровень пароля
QPWDMAXLEN	Минимальное число символов в пароле
QPWDMINLEN	Минимальное число символов в пароле
QPWDPOSDIF	Задает расположение символов в новом пароле
QPWDRQDDGT	Указывает, что пароль обязательно должен содержать цифру
QPWDRQDDIF	Указывает, должен ли новый пароль обязательно отличаться от предыдущего
QPWDRULES	Правила составления паролей
QPWDVLDPGM	Программа подтверждения паролей
QPWRDWNLMT	Максимальное время ожидания перед принудительным выключением
QRCLSPLSTG	Автоматическая очистка неиспользуемой памяти вывода на принтер
QRETSVRSEC	Индикатор сохранения идентификационных данных на сервере
QRMTSIGN	Удаленный вход в систему
QRMTSRVATR	Атрибут удаленной службы
QSCANFS	Сканирование файловых систем
QSCANFCTL	Управляющий элемент сканирования
QSCPFCONS	Возникла неполадка консоли
QSECURITY	Уровень защиты системы
QSETJOBATR	Задать атрибуты задания
QSFWERRLOG	Протокол ошибок ПО
QSHRMEMCTL	Разрешить использование общей или отображенной памяти с возможностью записи
QSPCENV	Среда пользователя по умолчанию
QSPLFACN	Действие буферного файла
QSRTSEQ	Последовательность сортировки
QSRVDMP	Протокол ошибок для неотслеживаемых аварийных сообщений
QSSLCSL	Список спецификаций шифров Secure Sockets Layer
QSSLCSLCTL	Управляющий элемент шифров Secure Sockets Layer
QSSLPCL	Протоколы Secure Sockets Layer
QSTRUPPGM	Задать программу запуска

Таблица 30. Атрибуты, которые можно отслеживать для переменных системных значений (продолжение)

Имя атрибута	Описание
QSTSMMSG	Просмотр сообщений о состоянии
QSYSLIBL	Список библиотек системы
QTIMSEP	Разделитель времени
QTSEPOOL	Указывает, следует ли перемещать интерактивные задания в другой пул оперативной памяти после окончания кванта времени
Примечание: Каждое системное значение трактуется как отдельная запись отслеживаемого ресурса. Поэтому тип ресурса и имена атрибутов совпадают.	

Таблица 31. Атрибуты, которые можно отслеживать для описаний накопителей на магнитной ленте

Имя атрибута	Описание
ASSIGN	Присвоить устройство при включении
MSGQ	Очередь сообщений
ONLINE	Включать при IPL
RSRCNAME	Имя ресурса
TEXT	Описание
UNLOAD	Выгружать устройство при выключении

Таблица 32. Атрибуты, которые можно отслеживать для описаний Token-Ring

Имя атрибута	Описание
ACTLANMGR	Активировать диспетчер LAN
ADPTADR	Локальный адрес адаптера
AUTOCRTCTL	Контроллер автоматического создания
AUTODLTCTL	Контроллер автоматического удаления
CMNRCYLMT	Лимиты восстановления
COSTBYTE	Относительная стоимость за бит для отправки и получения данных по линии
COSTCNN	Относительная стоимость подключения к линии
DUPLEX	Дуплекс
ELYTKNRLS	Ранний выпуск маркера
FCNADR	Функциональный адрес
LINESPEED	Быстродействие линии
LINKSPEED	Быстродействие канала связи
LOGCFGCHG	Записывать в протокол изменения в конфигурации
MAXCTL	Максимальное число контроллеров
MAXFRAME	Максимальные размеры кадра
MSGQ	Очередь сообщений
ONLINE	Включать при IPL
PRPDLY	Задержка распространения
RSRCNAME	Имя ресурса
SECURITY	Защита линии

Таблица 32. Атрибуты, которые можно отслеживать для описаний Token-Ring (продолжение)

Имя атрибута	Описание
SSAP	Информационный список Source service access point (SSAP)
TRNINBBDN	Сигнализирующая информация Token-Ring
TRNLOGLVL	Уровень ведения протоколов диспетчера TRLAN
TRNMGRMODE	Режим диспетчера TRLAN
TEXT	Описание линии Token-Ring
USRDFN1	Первый пользовательский
USRDFN2	Второй пользовательский
USRDFN3	Третий пользовательский
VRYWAIT	Ожидание включения

Таблица 33. Атрибуты, которые можно отслеживать для атрибутов TCP/IP

Имя атрибута	Описание
ARPTIMO	Тайм-аут кэша протокола преобразования адресов (ARP)
ECN	Включить явное уведомление о перегрузке (ECN)
IPDEADGATE	Функция обнаружения сбоев в работе шлюза IP
IPDTGFWD	Пересылка IP-дейтаграмм
IPPATHMTU	Поиск пути максимального блока передачи (MTU)
IPQOSBCH	Группирование дейтаграмм IP QoS
IPQOSEN	Разрешить IP QoS
IPQOSTMR	Преобразование таймера IP QoS
IPRSBTIMO	Тайм-аут сборки IP
IPSRCRTG	Маршрутизация источников IP
IPTTL	Время хранения в кэше IP (ограничение на пересылку)
LOGPCLERR	Регистрировать ошибки протоколов
NFC	Кэш сетевых файлов
TCPCLOTIMO	Тайм-аут паузы TCP
TCPCNNMSG	Сообщение о закрытии соединения TCP
TCPKEEPALV	Поддерживаемое соединение TCP
TCPMINRTM	Минимальное время TCP перед повторной передачей
TCPR1CNT	Число передач TCP R1
TCPR2CNT	Число передач TCP R2
TCPRCVBUF	Размер буфера приема TCP
TCPSNDBUF	Размер буфера отправки TCP
TCPURGPTR	Индикатор срочности TCP
UDPCKS	Контрольная сумма UDP
Примечание: Каждый атрибут TCP/IP трактуется как отдельная запись отслеживаемого ресурса. Поэтому тип ресурса и имена атрибутов совпадают.	

Таблица 34. Атрибуты, которые можно отслеживать для пользовательских профайлов

Имя атрибута	Описание
ACGCDE	Код учета ресурсов
ASTLVL	Уровень поддержки
ATNPGM	Программа Attention
CCSID	Идентификатор набора символов
CHRIDCTL	Управляющий элемент символьного идентификатора
CNTRYID	ИД страны или области
CURLIB	Текущая библиотека
DLVRY	Доставка
DSPSGNINF	Показать информацию о входе в систему
GID	Номер ИД группы
GRPAUT	Права доступа группы
GRPAUTTYP	Тип прав доступа группы
GRPPRF	Задан профайл группы
HOMEDIR	Домашний каталог
INLMNU	Начальное меню
INLPGM	Начальная программа
JOBID	Описание задания
KBDBUF	Буферизация нажатий клавиш
LANGID	ИД языка
LCLPDMGT	Локальное управление паролем
LMTCPB	Ограничить возможности
LMTDEVSSN	Ограничить сеансы одним устройством
LOCALE	Локаль
MAXSTG	Максимальный объем памяти
MSGQ	Очередь сообщений
OUTQ	Очередь вывода
OWNER	Владелец
PASSWORD	Пароль пользователя
PRTDEV	Принтер
PTYLMT	Наивысший приоритет планирования
PWDEXP	Ограничить срок действия пароля
PWDEXPITV	Срок действия пароля
SETJOBATR	Атрибуты локали задания
SEV	Фильтр кода серьезности
SPCAUT	Специальные права доступа
SPCENV	Специальная среда
SRTSEQ	Последовательность сортировки
STATUS	Состояние
SUPGRPPRF	Дополнительные группы
TEXT	Описание

Таблица 34. Атрибуты, которые можно отслеживать для пользовательских профайлов (продолжение)

Имя атрибута	Описание
UID	Номер ИД пользователя
USRCLS	Класс пользователя
USROPT	Опции пользователя

Отображение сообщений о записях отслеживаемых ресурсов:

С помощью графического интерфейса Службы ресурсов кластера можно просмотреть сообщения, связанные с записями отслеживаемых ресурсов.

Для просмотра сообщений о записях отслеживаемых ресурсов выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице службы ресурсов кластера нажмите кнопку **Работа с доменами управления**, чтобы увидеть список доменов управления кластером данного кластера.
5. На странице Домены управления щелкните на значке напротив домена управления кластером и выберите **Работа с типами отслеживаемых ресурсов**.

Примечание: Действие **Работа с типами отслеживаемых ресурсов** доступно, только если узел, с которым вы хотите работать, принадлежит домену управления кластером. Появится список типов отслеживаемых ресурсов.

6. В списке типов отслеживаемых ресурсов щелкните на значке, расположенном рядом с нужным типом, и выберите **Работа с записями отслеживаемых ресурсов**. Будет показан список объектов MRE.
7. Щелкните на значке контекстного меню рядом с объектом MRE, таким как пользовательский профайл или системное значение, и выберите **Показать сообщения**.

Управление переносимыми дисками

Переносимые диски - это независимые пулы дисков, которые настроены как часть группы ресурсов кластера устройств (CRG). Принадлежность данных и приложений, которые хранятся на переносимых дисках, можно изменять таким образом, чтобы их владельцем становилась другая система, определенная в CRG устройств. Технология переносимых дисков обеспечивает высокую готовность при запланированных и незапланированных простоях.

Запрет доступа к пулу дисков

При необходимости независимый пул дисков можно сделать недоступным (выключить его). До тех пор, пока независимый пул дисков не будет снова сделан доступным (включен), вы не сможете обратиться к дисками и объектам этого независимого пула дисков и связанной базы данных. Пул можно включить в той же или другой системе домена восстановления группы ресурсов кластера.

Важное замечание: Перед выключением независимого пула дисков необходимо завершить все задания, резервирующие ресурсы пула дисков. В разделе Освобождение зарезервированных заданиями ресурсов независимого пула дисков приведены инструкции по освобождению зарезервированных заданиями ресурсов.

В случае выключения пула дисков UDFS с помощью System i Navigator могут быть выданы сообщения, требующие ввода ответа в интерфейсе командной строки. System i Navigator не предупреждает о наличии ожидающих сообщений.

Для того чтобы сделать независимый пул дисков недоступным, выполните следующие действия:

1. В окне System i Navigator разверните запись **Мои соединения** (или активную среду).

2. Разверните систему System i и выберите **Настройка и обслуживание** → **Аппаратное обеспечение** → **Диски**.
3. Выберите **Пулы дисков**.
4. Щелкните правой кнопкой мыши на имени пула дисков, который требуется сделать недоступным, и выберите **Сделать недоступным**.
5. В открывшемся окне выберите **Сделать недоступным** для выключения пула дисков.

Пул дисков можно сделать недоступным из командной строки с помощью команды Изменить состояние конфигурации (VFYCFG).

Команда Показать состояние ASP (DSPASPSTS) позволяет определить обрабатываемый пул дисков.

С помощью API Управление доступом к ASP (QYASPCTLAA) запретите доступ отдельных процессов к ASP.

API Запустить операцию управления DASD (QYASSDMO) позволяет уменьшить продолжительность операции выключения пула дисков.

Включение переносимости аппаратного обеспечения

В среде высокой готовности i5/OS необходимо, сделать внешний блок расширения переносимым.

При использовании независимых пулов дисков в переносимой среде требуется предусмотреть переносимость связанного с ними аппаратного обеспечения. В зависимости от среды это может касаться стойки, блоков или IOP и связанных с ними ресурсов. Выполните следующие действия, связанные с переносимой средой.

Включение переносимости стойки или блока

Независимый пул дисков может содержать дисковые накопители в нескольких блоках расширения. При использовании автономного блока расширения, содержащего дисковые накопители, которые включены в независимый пул дисков, необходимо, чтобы блок расширения предоставлял доступ к другим системам. Это называется включением переносимости блока расширения. Если вам не требуется предоставлять другим системам доступ к автономному блоку расширения, необходимо сделать блок расширения частным.

Для включения переносимости стойки или блока выполните следующие действия:

1. В System i Navigator разверните **Соединения** (либо активную среду).
2. Разверните систему, которую требуется просмотреть, выберите **Настройка и обслуживание** → **Аппаратное обеспечение** → **Дисковые накопители** → **По расположению** и выберите стойку или дисковый накопитель, которые требуется сделать переносимыми.
3. Щелкните правой кнопкой мыши на выбранной стойке или дисковом накопителе и выберите **Сделать переносимым**.
4. Следуйте инструкциям в появившемся окне диалога.

Включение переносимости IOP

Для того чтобы обеспечить переносимость IOP, главный узел должен быть *совместным владельцем* шины с IOP, управляющим дисковыми накопителями, которые требуется сделать переносимыми. Для этой шины резервный узел должен быть *пользователем общей шины*. Более подробная информация приведена в разделе Динамический перенос IOP между разделами.

Для этого необходим пользовательский профайл сервисных средств с правами на администрирование функции Разделы системы, входящей в состав Специальных сервисных средств (DST). Дополнительные сведения о получении прав доступа к логическому разделу приведены в разделе Права доступа к логическим разделам.

Для того чтобы изменить тип владельца шины с помощью Централизованного управления, выполните следующие действия:

1. В System i Navigator разверните **Соединения** (либо активную среду).
2. Выберите основной раздел системы.
3. Разверните значок **Настройка и обслуживание** и выберите пункт **Логические разделы**.
4. Щелкните правой кнопкой мыши на пункте **Логические разделы** и выберите **Настроить разделы**.
5. В окне Настроить логические разделы щелкните правой кнопкой мыши на шине, тип владельца которой требуется изменить, и выберите пункт **Свойства**.
6. Выберите страницу **Разделы**.
7. Выберите раздел, которому принадлежит шина, в окне **Логические разделы - владельцы**, а затем выберите тип владельца в поле **Совместное использование**. Если раздел владеет шиной совместно с другими разделами, то в списке будут показаны все разделы, совместно использующие шину. Для получения дополнительной информации об этих опциях нажмите кнопку Справка.
8. Нажмите **ОК**.

Включение переносимости пула ввода-вывода с помощью Консоли аппаратного обеспечения

Если для управления логическими разделами вы применяете Консоль аппаратного обеспечения, то для включения переносимости независимого пула дисков между разделами создайте пул ввода-вывода, в который включены IOP, IOA и все подключенные ресурсы. Предоставьте права доступа каждому разделу, который требуется назначить владельцем независимого пула дисков, задав пул ввода-вывода в профайле каждого раздела.

Для создания пула ввода-вывода, который является переносимым между разделами, выполните следующие действия:

1. Откройте окно Свойства профайла логического раздела для того чтобы изменить свойства профайла и задать ресурсы пула ввода-вывода.
2. Щелкните на вкладке **Физические устройства ввода-вывода**.
3. В столбце устройств ввода-вывода профайла разверните шину, содержащую IOP, который требуется сделать переносимым.
4. Выберите IOP, который требуется назначить для пула ввода-вывода. IOP должен быть отмечен как *желательный* (без отметки в столбце **Обязательный**).
5. Щелкните на столбце пула ввода-вывода таким образом, чтобы в строке IOP, который требуется назначить для пула ввода-вывода, появился курсор, и введите номер пула ввода-вывода.
6. Повторите эти шаги для каждого IOA и ресурса, которыми управляет IOP, назначаемый для пула ввода-вывода.
7. Нажмите **ОК**.

Связывание пула ввода-вывода с разделами

После добавления ресурсов в пул ввода-вывода выполните следующие действия для того чтобы связать пул ввода-вывода с каждым из остальных разделов, которые смогут быть назначены владельцами независимого пула дисков в переносимой среде.

1. Откройте окно Свойства профайла логического раздела для того чтобы изменить свойства профайла каждого из остальных разделов, которым потребуются права доступа к независимому пулу дисков.
2. Щелкните на вкладке **Физические устройства ввода-вывода**.
3. Нажмите кнопку **Дополнительно**.
4. В окне Пулы ввода-вывода в поле **Добавляемые пулы ввода-вывода** введите номер пула, связанного с ресурсами, которые требуется сделать переносимыми вместе с независимым пулом дисков.
5. Нажмите кнопку **Добавить**, а затем - **ОК**.

Для того чтобы применить изменения в профайле пула ввода-вывода выполните следующие действия для каждого раздела, профайл которого был изменен:

1. Завершите работу раздела. Обратитесь к разделу Перезапуск и завершение работы i5/OS в логическом разделе.
2. Для применения изменений запустите логический раздел, активировав его профайл.

Понятия, связанные с данным

Динамический перенос процессоров ввода-вывода между разделами

Права доступа к логическим разделам

Пул ввода-вывода

Задачи, связанные с данной

Изменение свойств профайла раздела

Активация профайла раздела

Перезапуск и завершение работы i5/OS™ в логическом разделе

| Выполнение приостановки независимого пула дисков

| В решении высокой готовности i5/OS независимые пулы дисков используются для хранения устойчивых данных и приложений. Для некоторых системных функций, например, выполнения резервного копирования, необходимо временно приостановить изменения данных на время операции.

| Для сокращения времени, необходимого для приостановки независимого пула дисков, может потребоваться заблокировать очереди пакетных заданий, завершить работу некоторых подсистем или отправить прерывающее сообщение интерактивным пользователям с рекомендацией отложить новую работу.

| Для приостановки независимого пула дисков выполните следующие действия.

| В командной строке введите следующую команду: CHGASPACT ASPDEV(имя) OPTION(*SUSPEND) SSPTIMO(30) SSPTIMOACN(*CONT),, где *имя* - это имя независимого пула дисков, который требуется приостановить. Эта команда указывает на приостановку независимого пула диска с 30-секундным тайм-аутом и продолжение выполнения следующего шага даже в случае превышения лимита тайм-аута.

Возобновление работы независимого пула дисков

Если независимый пул дисков в среде высокой готовности i5/OS был приостановлен для выполнения операций резервного копирования, потребуется возобновить его работу, чтобы обеспечить обновление данных, измененных во время приостановки.

Для возобновления работы независимого пула дисков выполните следующие действия:

В командной строке введите следующую команду: CHGASPACT ASPDEV(имя) OPTION(*RESUME),, где *имя* - это имя независимого пула дисков, работу которого следует возобновить.

Распределенное зеркальное копирование

Распределенное зеркальное копирование может реализовываться на основе трех технологий: географическое зеркальное копирование, синхронное зеркальное копирование и глобальное зеркальное копирование. Эти технологии распределенной зеркальной защиты обеспечивают восстановление критических данных после аварий благодаря наличию резервных копий дисков рабочих систем в других расположениях.

Управление географической зеркальной защитой

Приведенная здесь информация поможет вам в управлении географической зеркальной защитой.

Географическая зеркальная защита представляет собой подфункцию распределенной по сайтам зеркальной защиты, при которой создается зеркальная копия данных на независимых пулах дисков в среде i5/OS.

Выключение географической зеркальной защиты:

Перед тем, как прервать передачу данных по протоколу TCP (например, для перевода системы в состояние с ограничениями), необходимо выключить географическую зеркальную защиту. Данное действие позволяет временно остановить зеркальную защиту систем, входящих в состав решения высокой готовности.

Если зеркальная защита выключена, то в течение этого времени любые изменения, внесенные в рабочей копии независимого пула дисков, не будут передаваться в зеркальную копию.

Примечание: При возобновлении работы географической зеркальной защиты необходимо выполнить полную синхронизацию рабочих и зеркальных копий. Если географическая зеркальная защита была выключена без отслеживания изменений, то необходимо выполнить полную синхронизацию. Синхронизация может занять значительное время.

| **Выключение географической зеркальной защиты с помощью IBM Systems Director Navigator for i5/OS**

Для того чтобы приостановить географическую зеркальную защиту с помощью IBM Systems Director Navigator for i5/OS, выполните следующие действия:

- | 1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
- | 2. Войдите в систему, указав пользовательский профайл и пароль.
- | 3. Выберите **Настройка и обслуживание** в окне IBM Systems Director Navigator for i5/OS.
- | 4. Выберите **Пулы дисков**.
- | 5. Выберите рабочую копию пула дисков, для которого требуется приостановить географическую зеркальную защиту.
- | 6. В меню **Выбрать действие** выберите **Сеансы**.
- | 7. Выберите сеанс, который требуется приостановить.
- | 8. В меню **Выбрать действие** выберите **Приостановить с отслеживанием** или **Приостановить без отслеживания**.

Выключение географической зеркальной защиты с помощью System i Navigator

| Для того чтобы приостановить географическую зеркальную защиту с помощью System i Navigator, выполните следующие действия:

- | 1. В окне System i Navigator разверните запись **Мои соединения** (или активную среду).
- | 2. Разверните систему с рабочей копией пула дисков, для которого вы хотите приостановить процедуру географической зеркальной защиты.
- | 3. Разверните **Настройка и обслуживание** → **Аппаратное обеспечение** → **Дисковые накопители** → **Пулы дисков**.
- | 4. Щелкните правой кнопкой мыши на рабочей копии пула дисков и выберите **Географическая зеркальная защита** → **Приостановить географическую зеркальную защиту**.

Если работа географической зеркальной защиты прервана с мониторингом, то система будет отслеживать изменения, вносимые в пулы дисков. Такой подход позволяет сократить продолжительность процесса синхронизации путем частичной синхронизации после возобновления работы географической зеркальной защиты. В случае превышения размера области мониторинга после возобновления работы географической зеркальной защиты выполняется полная синхронизация.

Примечание: При возобновлении работы географической зеркальной защиты без мониторинга изменений необходимо выполнить полную синхронизацию рабочих и зеркальных копий. Если географическая зеркальная защита была приостановлена с мониторингом изменений, то выполняется только частичная синхронизация. Полная синхронизация может занять несколько часов. Время, необходимое для синхронизации, зависит объема обрабатываемых данных, пропускной способности соединений TCP/IP и числа линий связи, выделенных для географической зеркальной защиты.

Возобновление географической зеркальной защиты:

Если географическая зеркальная защита была приостановлена, ее необходимо возобновить для активации зеркального копирования между рабочими данными и их зеркальной копией.

Примечание: После возобновления географической зеркальной защиты рабочая и зеркальная копии синхронизируются параллельно выполнению географической зеркальной защиты. Синхронизация может занять значительное время. Если синхронизация прерывается из-за недоступности пула дисков, она будет продолжена после того, как пул дисков снова станет доступным. В случае продолжения прерванной синхронизации первое сообщение (CPI0985D) указывает, что синхронизация выполнена на 0%.

| **Возобновление географической зеркальной защиты с помощью IBM Systems Director Navigator for i5/OS**

Для возобновления географической зеркальной защиты с помощью IBM Systems Director Navigator for i5/OS выполните следующие действия:

- | 1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
- | 2. Войдите в систему, указав пользовательский профайл и пароль.
- | 3. Выберите **Настройка и обслуживание** в окне IBM Systems Director Navigator for i5/OS.
- | 4. Выберите **Пулы дисков**.
- | 5. Выберите рабочую копию **Пула дисков**, работу которой следует продолжить.
- | 6. В меню **Выбрать действия** выберите опцию **Сеансы**.
- | 7. Выберите сеанс для продолжения.
- | 8. В меню **Выбрать действия** выберите опцию **Продолжить**.

| **Возобновление географической зеркальной защиты с помощью System i Navigator**

| Для возобновления географической зеркальной защиты с помощью System i Navigator выполните следующие действия:

- | 1. В System i Navigator разверните **Соединения** (либо активную среду).
- | 2. Разверните систему, содержащую рабочую копию пула дисков, для которой следует продолжить географическую зеркальную защиту.
- | 3. Разверните **Настройка и обслуживание** → **Аппаратное обеспечение** → **Дисковые накопители** → **Пулы дисков**.
- | 4. Щелкните правой кнопкой мыши на **Пуле дисков**, работу которого следует продолжить, и выберите **Географическая зеркальная защита** → **Продолжить географическую зеркальную защиту**.

Для сокращения времени, в течение которого пул дисков недоступен, используйте API Запуск операции управления DASD (QYASSDMO).

Отсоединение зеркальной копии:

Если вы используете географическую зеркальную защиту и вам необходимо получить доступ к зеркальной копии для выполнения операций сохранения, сбора и анализа данных или создания отчетов, необходимо отсоединить зеркальную копию от рабочей копии.

Отсоединение осуществляется через доступ к рабочей копии пула дисков.

Примечание: После дальнейшего присоединения отсоединенной зеркальной копии потребуется полная синхронизация рабочей и зеркальной копий. Такая синхронизация может занять много времени.

| **Отсоединение зеркальной копии с помощью Навигатора IBM Systems Director для i5/OS**

| Для отсоединения зеркальной копии с помощью Навигатора IBM Systems Director для i5/OS выполните следующие действия:

- | 1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
- | 2. Войдите в систему, указав пользовательский профайл и пароль.

- | 3. Выберите **Настройка и службы** в окне Навигатора IBM Systems Director для i5/OS.
- | 4. Выберите **Пулы дисков**.
- | 5. Выберите рабочую копию **Пула дисков**, которую необходимо отсоединить.
- | 6. В меню **Выбор действий** выберите **Сеансы**.
- | 7. Выберите сеанс, который необходимо отсоединить.
- | 8. В меню **Выбор действий** выберите **Отсоединить с мониторингом** или **Отсоединить без мониторинга**.

| **Отсоединение зеркальной копии с помощью System i Navigator**

Рекомендуется сделать пул диска недоступным для того, чтобы удостовериться, что рабочая копия не будет изменена во время выполнения отсоединения.

- | Для отсоединения зеркальной копии с помощью System i Navigator выполните следующие действия:
 1. В System i Navigator разверните **Соединения** (либо активную среду).
 2. Разверните систему, владеющую рабочей копией пула дисков, от которого необходимо отсоединить зеркальную копию.
 3. Разверните **Настройка и службы** → **Аппаратное обеспечение** → **Дисковые накопители** → **Пулы дисков**.
 4. Щелкните правой кнопкой мыши на рабочей копии **Пула дисков**, которую вы хотите отсоединить, и выберите **Географическая зеркальная защита** → **Отсоединить зеркальную копию**.

Если невозможно щелкнуть на пункте **Географическая зеркальная защита** → **Отсоединить зеркальную копию**, поскольку он не активен, это означает, что зеркальная копия не синхронизирована с рабочей копией. В этом случае, прежде чем будет возможно отсоединить зеркальную копию, необходимо возобновить работу географической зеркальной защиты, включить пул дисков и провести синхронизацию рабочей и зеркальной копий.

Прежде чем сделать доступной отсоединенную зеркальную копию, необходимо создать второе, уникальное, описание устройства для независимого ASP, которое будет отличать его от рабочей копии. Отдельное описание устройства для зеркальной копии предупреждает появление двух экземпляров одной и той же базы данных в сети. Оно также упростит работу вне System i Navigator. Описание отсоединенной зеркальной копии устройства используется для того, чтобы сделать ее доступной.

Присоединение зеркальной копии:

После завершения работы с отсоединенной зеркальной копией необходимо ее присоединить, чтобы возобновить применение географической зеркальной защиты.

Для присоединения отсоединенной зеркальной копии воспользуйтесь рабочей копией пула дисков. Отсоединенная зеркальная копия должна быть недоступна при ее присоединении к рабочей копии.

Примечание: При присоединении отсоединенной зеркальной копии требуется полная синхронизация между рабочей и зеркальной копиями. Синхронизация может занять значительное время.

| **Присоединение зеркальной копии с помощью IBM Systems Director Navigator for i5/OS**

- | Для присоединения зеркальной копии с помощью IBM Systems Director Navigator for i5/OS выполните следующие действия:
 - | 1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
 - | 2. Войдите в систему, указав пользовательский профайл и пароль.
 - | 3. Выберите **Настройка и обслуживание** в окне IBM Systems Director Navigator for i5/OS.
 - | 4. Выберите **Пулы дисков**.
 - | 5. Выберите рабочую копию **Пула дисков**, которую следует приостановить.

- | 6. В меню **Выбрать действия** выберите опцию **Сеансы**.
- | 7. Выберите сеанс для приостановки.
- | 8. В меню **Выбрать действия** выберите опцию **Присоединить**.

| Присоединение зеркальной копии с помощью System i Navigator

| Для присоединения зеркальной копии с помощью System i Navigator выполните следующие действия:

1. В System i Navigator разверните **Соединения** (либо активную среду).
2. Разверните систему, содержащую рабочую копию пула дисков, к которой следует присоединить отсоединенную зеркальную копию.
3. Разверните **Настройка и обслуживание** → **Аппаратное обеспечение** → **Дисковые накопители** → **Пулы дисков**.
4. Щелкните правой кнопкой мыши на рабочей копии **Пула дисков**, которую следует подключить, и выберите **Географическая зеркальная защита** → **Присоединить зеркальную копию**.

Удаление географической зеркальной защиты:

Если вы больше не хотите применять географическую зеркальную защиту для определенного пула дисков или группы пулов дисков вы можете выбрать опцию **Удалить географическую зеркальную защиту**. После удаления географической зеркальной защиты система перестает осуществлять географическую зеркальную защиту и удаляет зеркальную копию пулов дисков из узлов на сайте зеркального копирования.

Для удаления географической зеркальной защиты пул дисков должен находиться в автономном режиме.

Для удаления географической зеркальной защиты выполните следующие действия:

1. В System i Navigator разверните **Соединения** (либо активную среду).
2. Разверните систему, с которой вы хотите ознакомиться, а затем - **Настройка и службы** → **Аппаратное обеспечение** → **Дисковые накопители** → **Пулы дисков**.
3. Щелкните правой кнопкой мыши на рабочей копии **Пула дисков**, которую вы хотите удалить, и выберите **Географическая зеркальная защита** → **Удалить географическую зеркальную защиту**.
4. Обновите конфигурацию кластера следующим образом:
 - a. Удалите узлы, связанные с зеркальной копией, из домена восстановления группы ресурсов кластера (CRG).
 - b. Удалите имя сайта и IP-адреса портов данных из оставшихся узлов кластера.

Задачи, связанные с данной

“Удаление узлов” на стр. 123

- | Иногда возникает необходимость узел из кластера, если выполняется обновление этого узла или если
- | узел более не участвует в среде высокой готовности i5/OS.

Изменение свойств географической зеркальной защиты:

В разделе описано изменение сведений о географической зеркальной защите и описаний соответствующих копий.

Изменение свойств географической зеркальной защиты с помощью Навигатора IBM Systems Director для i5/OS

Для изменения сеанса географической зеркальной защиты с помощью Навигатора IBM Systems Director для i5/OS выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Настройка и обслуживание** в окне Навигатора IBM Systems Director для i5/OS.

4. Выберите опцию **Пулы дисков**.
5. Выберите пул дисков, связанный с сеансом.
6. В меню **Выбрать действие** выберите опцию **Сеансы**.
7. Выберите сеанс.
8. В меню **Выбрать действие** выберите опцию **Свойства**. Для изменения описания соответствующей копии выберите описание копии и нажмите кнопку **Правка**.

Изменение свойств географической зеркальной защиты с помощью Навигатора System i

Для изменения сеанса географической зеркальной защиты с помощью Навигатора System i выполните следующие действия:

1. В System i Navigator разверните **Соединения** (либо активную среду).
2. Разверните пункт, соответствующий системе, которая является владельцем рабочей копии пула дисков с географической зеркальной защитой, связанных с сеансом географической зеркальной защиты, для которого требуется изменить атрибуты, и откройте **Настройка и обслуживание** → **Аппаратное обеспечение** → **Дисковые накопители** → **Пулы дисков**.
3. Щелкните правой кнопкой мыши на **Пуле дисков**, для которого требуется изменить атрибуты, и выберите **Сеансы** → **Открыть**.
4. Щелкните правой кнопкой мыши на рабочей копии **Сеанса**, для которого требуется изменить атрибуты, и выберите опцию **Свойства**. Для изменения описания соответствующей копии выберите описание копии и нажмите кнопку **Изменить**.

Управление сеансами синхронного зеркального копирования

В среде высокой готовности i5/OS, в которой применяется технология синхронного зеркального копирования IBM System Storage, необходимо настроить сеанс синхронного зеркального копирования между системами i5/OS и внешними дисковыми накопителями, для которых настроено синхронное зеркальное копирование. Этими сеансами можно будет управлять из системы.

Приостановка сеансов синхронного зеркального копирования:

Сеанс синхронного зеркального копирования может потребоваться приостановить для обслуживания системы.

Для того чтобы приостановить сеанс синхронного зеркального копирования, выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите **Настройка и обслуживание** в окне IBM Systems Director Navigator for i5/OS.
4. Выберите **Пулы дисков**.
5. Выберите пул дисков, который необходимо приостановить.
6. В меню **Выбрать действие** выберите **Сеансы**.
7. Выберите сеанс, который требуется приостановить.
8. В меню **Выбрать действие** выберите **Приостановить**.

Возобновление сеансов синхронного зеркального копирования:

После выполнения обычных операций, например, после техобслуживания системы, необходимо продолжить сеанс синхронного зеркального копирования, чтобы восстановить высокую готовность.

Для продолжения сеанса синхронного зеркального копирования выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.

3. Выберите **Настройка и обслуживание** в окне IBM Systems Director Navigator for i5/OS.
4. Выберите **Пулы дисков**.
5. Выберите пул дисков, работа которого приостановлена.
6. В меню **Выбрать действия** выберите опцию **Сеансы**.
7. Выберите сеанс, работа которого приостановлена.
8. В меню **Выбрать действия** выберите опцию **Продолжить**.

Удаление сеанса синхронного зеркального копирования:

Можно удалить сеанс синхронного зеркального копирования, чтобы в дальнейшем не использовать его для высокой готовности и восстановления после аварий.

Для удаления сеанса синхронного зеркального копирования выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите **Настройка и службы** в окне Навигатора IBM Systems Director для i5/OS.
4. Выберите **Пулы дисков**.
5. Выберите пул диска, связанный с сеансом, который необходимо удалить.
6. В меню **Выбор действий** выберите **Сеансы**.
7. Выберите сеанс, который необходимо удалить.
8. В меню **Выбрать действия** выберите **Удалить**.

Просмотр свойств синхронного зеркального копирования:

В этом разделе описана работа с сеансом зеркального копирования для изменения связанных описаний копирования.

Для того чтобы изменить свойства зеркального копирования в IBM Systems Director Navigator for i5/OS, выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите пункт **Настройка и обслуживание** в окне IBM Systems Director Navigator for i5/OS.
4. Выберите **Пулы дисков**.
5. Выберите пул дисков, связанный с сеансом.
6. В меню **Выберите действие** выберите пункт **Сеансы**.
7. Выберите сеанс.
8. В меню **Выберите действие** выберите пункт **Свойства**. Для того чтобы изменить связанное описание копирования, выберите его и нажмите кнопку **Изменить**.

Управление глобальным зеркальным копированием

В среде высокой готовности i5/OS, которая использует технологию глобального зеркального копирования IBM System Storage, необходимо настроить сеанс глобального зеркального копирования между системами i5/OS и внешними дисковыми накопителями с использованием глобального зеркального копирования. Этими сеансами можно управлять из системы.

Приостановка сеансов глобального зеркального копирования:

Сеанс глобального зеркального копирования может потребоваться приостановить для обслуживания системы.

Для того чтобы приостановить сеанс глобального зеркального копирования, выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите **Настройка и обслуживание** в окне IBM Systems Director Navigator for i5/OS.
4. Выберите **Пулы дисков**.
5. Выберите пул дисков, который необходимо приостановить.
6. В меню **Выбрать действие** выберите **Сеансы**.
7. Выберите сеанс, который требуется приостановить.
8. В меню **Выбрать действие** выберите **Приостановить**.

Возобновление сеансов глобального зеркального копирования:

После выполнения обычных операций, например, после техобслуживания системы, необходимо продолжить сеанс глобального зеркального копирования, чтобы восстановить высокую готовность.

Для продолжения сеанса глобального зеркального копирования выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите **Настройка и обслуживание** в окне IBM Systems Director Navigator for i5/OS.
4. Выберите **Пулы дисков**.
5. Выберите пул дисков, работа которого приостановлена.
6. В меню **Выбрать действия** выберите опцию **Сеансы**.
7. Выберите сеанс, работа которого приостановлена.
8. В меню **Выбрать действия** выберите опцию **Продолжить**.

Удаление сеансов глобального зеркального копирования:

Можно удалить сеанс глобального зеркального копирования, чтобы в дальнейшем не использовать его для высокой готовности и восстановления после аварий.

Для удаления сеанса глобального зеркального копирования выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите **Настройка и службы** в окне Навигатора IBM Systems Director для i5/OS.
4. Выберите **Пулы дисков**.
5. Выберите пул диска, связанный с сеансом, который необходимо удалить.
6. В меню **Выбор действий** выберите **Сеансы**.
7. Выберите сеанс, который необходимо удалить.
8. В меню **Выбрать действия** выберите **Удалить**.

Изменение свойств сеанса глобального зеркального копирования:

В разделе описано изменение описаний копий, связанных с сеансом глобального зеркального копирования с помощью Навигатора.

Для изменения свойств глобального зеркального копирования с помощью Навигатора IBM Systems Director для i5/OS выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.

3. Выберите опцию **Настройка и обслуживание** в окне Навигатора IBM Systems Director для i5/OS.
4. Выберите опцию **Пулы дисков**.
5. Выберите пул дисков, связанный с сеансом.
6. В меню **Выбрать действие** выберите опцию **Сеансы**.
7. Выберите сеанс.
8. В меню **Выбрать действие** выберите опцию **Свойства**. Для изменения описания соответствующей копии выберите описание копии и нажмите кнопку **Правка**.

Управление FlashCopy

FlashCopy - это технология IBM System Storage, которая позволяет создавать синхронные копии внешних дисковых накопителей. В решениях высокой готовности i5/OS с использованием синхронного или глобального зеркального копирования можно использовать FlashCopy для уменьшения объема копирования, создав копию данных, из которой затем будет сделана резервная копия на носителе. Для использования FlashCopy необходимо создать сеанс между системой и внешними накопителями.

Настройка сеанса FlashCopy

Для сред высокой готовности i5/OS, использующих технологию IBM System Storage, можно настроить сеанс FlashCopy для создания синхронной копии данных.

Со сведениями об использовании FlashCopy для IBM System Storage DS6000 можно ознакомиться в IBM System Storage DS6000 Information Center. Со сведениями об использовании для IBM System Storage DS8000, можно ознакомиться в IBM System Storage DS8000 Information Center.

Для настройки сеанса FlashCopy выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите **Конфигурация и служба** в окне Навигатор IBM Systems Director для i5/OS.
4. Выберите **Пулы дисков**.
5. Выберите пул дисков, который должен применяться как исходная копия.
6. В меню **Выбор действий** выберите **Создать сеанс**.
7. Для завершения задачи следуйте инструкциям мастера.

Обновление FlashCopy

Обновить сеанс FlashCopy можно при синхронизации томов FlashCopy на внешних жестких дисках IBM System Storage. Синхронизация позволяет создавать копии без копирования всего тома. Этот процесс может происходить только при условии постоянной связи, благодаря которому диск постоянно следит за обновлениями исходного и целевого томов. При этом исходный и целевой тома остаются взаимосвязанными после завершения фоновое копирования. Сеанс FlashCopy, созданный в i5/OS, предоставляет средства для управления и контроля деятельности, касающейся FlashCopy на блоках IBM System Storage.

Для обновления сеанса FlashCopy выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите опцию **Настройка и обслуживание** в окне Навигатора IBM Systems Director для i5/OS.
4. Выберите опцию **Пулы дисков**.
5. Выберите пул дисков, связанный с обновляемым сеансом.
6. В меню **Выбрать действие** выберите опцию **Сеансы**.
7. Выберите сеанс для обновления.
8. В меню **Выбрать действие** выберите опцию **Обновить FlashCopy**.

Присоединение FlashCopy

Можно присоединить сеанс FlashCopy.

Для присоединения сеанса FlashCopy выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите **Настройка и обслуживание** в окне IBM Systems Director Navigator for i5/OS.
4. Выберите **Пулы дисков**.
5. Выберите пул дисков, связанный с сеансом, который следует присоединить.
6. В меню **Выбрать действия** выберите опцию **Сеансы**.
7. Выберите сеанс для присоединения.
8. В меню **Выбрать действия** выберите опцию **Присоединить FlashCopy**.

Отсоединение FlashCopy

Можно отсоединить целевой том от исходного для определенного сеанса FlashCopy.

Для отсоединения целевых томов от исходного для определенного сеанса FlashCopy выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите **Настройка и службы** в окне Навигатора IBM Systems Director для i5/OS.
4. Выберите **Пулы дисков**.
5. Выберите пул диска, связанный с сеансом, который необходимо отсоединить.
6. В меню **Выбор действий** выберите **Сеансы**.
7. Выберите сеанс, для которого необходимо отсоединить целевой и исходный тома.
8. В меню **Выбор действий** выберите **Отсоединить FlashCopy**.

Удаление FlashCopy

Удаление сеанса FlashCopy.

Для удаления сеанса FlashCopy выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите **Настройка и службы** в окне Навигатора IBM Systems Director для i5/OS.
4. Выберите **Пулы дисков**.
5. Выберите пул диска, связанный с сеансом, который необходимо удалить.
6. В меню **Выбор действий** выберите **Сеансы**.
7. Выберите сеанс, который необходимо удалить.
8. В меню **Выбрать действия** выберите **Удалить**.

Восстановление данных из FlashCopy

После выполнения FlashCopy для модулей IBM System Storage, можно восстанавливать данные из целевого тома в исходный в случае выхода из строя исходной копии данных. Для этого необходимо инвертировать сеанс FlashCopy, созданный в i5/OS. Однако в обратном сеансе данные копируются из цели обратно в источник, и таким образом источник возвращается к более ранней версии.

Внимание: При инверсии сеанса FlashCopy отменяются изменения в исходной копии посредством копирования данных из целевой копии обратно в исходную. Таким образом, исходная копия возвращается к более раннему моменту времени.

Для инверсии сеанса FlashCopy выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите **Настройка и обслуживание** в окне IBM Systems Director Navigator for i5/OS.
4. Выберите **Пулы дисков**.
5. Выберите пул дисков исходной копии.
6. В меню **Выбрать действия** выберите опцию **Открыть сеансы**.
7. Выберите сеанс.
8. В меню **Выбрать действия** выберите опцию **Инvertировать FlashCopy**.

Изменение свойств FlashCopy

Для изменения описаний связанных копий необходимо отобразить сведения о сеансе FlashCopy.

Для изменения сведений о сеансе FlashCopy выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профайл и пароль.
3. Выберите **Настройка и службы** в окне Навигатора IBM Systems Director для i5/OS.
4. Выберите **Пулы дисков**.
5. Выберите пул диска, связанный с сеансом.
6. В меню **Выбор действий** выберите **Сеансы**.
7. Выберите сеанс.
8. В меню **Выбрать действия** выберите **Свойства**. Для изменения описания связанной копии выберите описание копии и нажмите кнопку **Изменить**.

Устранение неполадок решения высокой готовности

После настройки решения высокой готовности i5/OS могут возникнуть неполадки, связанные с различными технологиями, включая кластеры и распределенную по сайтам зеркальную защиту.

Устранение неполадок кластера

Процедуры устранения типичных неполадок, возникающих при работе с кластерами.

Кластеры, как и любые другие аппаратно-программные решения, подвержены неполадкам. В этом разделе приведена информация о том, какие неполадки могут возникать при работе с кластерами.

Проверка работоспособности кластера

Устранение неполадок следует начать с диагностики.

Кластеры, как и любые другие аппаратно-программные решения, подвержены неполадкам. Если у вас возникло впечатление, что кластер работает неправильно, то сначала следует проверить его работоспособность.

- **Определите, работает ли в системе служба ресурсов кластера.**

| Для того чтобы определить, работает ли кластер, нужно проверить наличие заданий QCSTCTL и
| QCSTCRGM в списке заданий системы. Если эти задания активны, то служба ресурсов кластера работает.
| Проверить наличие заданий можно с помощью функции управления заданиями IBM Director Navigator for
| i5/OS или System i Navigator или с помощью команды WRKACTJOB (Работа с активными заданиями).
| Кроме того, можно посмотреть текущее состояние кластера с помощью команды DSPCLUINF (Показать
| информацию о кластере) .

— Помимо этих, кластер может использовать и другие задания. В разделе Задания кластера приведена информация о формате заданий службы ресурсов кластера.

- **Определите причину выдачи сообщения CPFBB26.**

Сообщение . . . : Службы ресурсов кластера выключены или не отвечают.
Причина . . . : Службы ресурсов кластера выключены или не могут ответить на запрос,
поскольку ресурс недоступен или поврежден.

Возможно, не активно задание CRG или кластер. Проверьте состояние узла с помощью команды DSPCLUINF (Показать информацию о кластере). Если узел не активен, то запустите его. В противном случае проверьте наличие неполадок CRG.

Найдите задание CRG в списке системных заданий. Для этого воспользуйтесь функцией управления заданиями IBM Director Navigator for i5/OS или System i Navigator либо командой WRKACTJOB (Работа с активными заданиями). Кроме того, информацию о состоянии конкретной группы ресурсов кластера можно просмотреть, указав ее имя в команде DSPCRGINF (Показать информацию о CRG). Если задание CRG не выполняется, то определения причины его завершения обратитесь к протоколу задания. После устранения неполадки перезапустите задание CRG с помощью команды CHGCLURCY (Изменить состояние восстановления кластера) или путем перезапуска кластера на узле.

- **Попытайтесь найти сообщения об ошибках.**

- Убедитесь, что для просмотра доступны все сообщения, связанные с командой кластера. Для этого нажмите клавишу F10, которая отвечает за переключение между режимами "Показать подробные сообщения" и "Скрыть подробные сообщения". Выберите режим отображения подробных сообщений и просмотрите их для определения необходимости выполнения дополнительных действий.
- Просмотрите, нет ли в очереди QSYSOPR сообщений-вопросов, ожидающих ответа.
- Просмотрите, нет ли в очереди QSYSOPR сообщений об ошибках, связанных с кластером. Идентификаторы большинства таких сообщений лежат в диапазоне CPFBB00-CPFBBFF.
- Проверьте, нет ли сообщений о неполадках кластера в протоколе хронологии (команда CL DSPLOG). Идентификаторы большинства таких сообщений лежат в диапазоне CPFBB00-CPFBBFF.

- **Проверьте протоколы заданий кластера на наличие сообщений о серьезных ошибках.**

Обычно для этих заданий установлен уровень (4 0 *SECLVL) ведения протокола, а на этом уровне в протокол заносятся все сообщения об ошибках. Проверьте, правильно ли задан уровень ведения протокола для этих заданий кластера и заданий программ выхода. Даже если кластер не запущен, вы можете просмотреть буферные файлы заданий кластера и заданий программ выхода.

- **Если кластер не отвечает на запросы, проанализируйте стеки вызовов заданий кластера.**

Посмотрите, есть ли в очередях программы вида DEQW (ожидание освобождения очереди). Если такие программы есть, просмотрите все нити этих программ и выясните, есть ли у каких-либо из них getSpecialMsg в стеке вызова.

- **Проверьте содержимое протоколов на наличие записей вертикального лицензионного внутреннего кода (VLIC).**

Это должны быть записи с главным кодом 4800.

- **С помощью команды NETSTAT определите состояние среды связи.**

Команда NETSTAT позволяет получить сведения о состоянии маршрутов TCP/IP, интерфейсов, соединений TCP и портов UDP.

- С помощью опции 1 команды NETSTAT (Работа с состоянием интерфейсов TCP/IP) убедитесь в том, что IP-адреса, выделенные кластеру, находятся в состоянии 'Активен'. Убедитесь, что активен циклический адрес (127.0.0.1).
- С помощью опции 3 команды NETSTAT (Работа с состоянием соединений TCP/IP) просмотрите номера портов (F14). Локальный порт 5550 должен находиться в состоянии 'Прослушивание'. Если в списке активных заданий есть задание QTOGINTD (пользователь QTCP), то этот порт должен был быть открыт командой STRTCPSVR *INETD. Если на узле запущена служба ресурсов кластера, то локальный порт 5551 должен быть открыт и находиться в состоянии '*UDP'. Если служба ресурсов кластера не запущена, порт 5551 должен быть закрыт (если он будет открыт, то вам не удастся запустить на этом узле службу ресурсов кластера).
- Воспользуйтесь командой ping. Если вы пытаетесь запустить узел кластера, с которым нет связи, вы получите внутреннюю ошибку кластера (CPFBB46).

| Сбор данных для восстановления кластера

| Для сбора полной информации о кластере можно воспользоваться командой Работа с кластером (WRKCLU). Эта информация может помочь при устранении неполадок.

| Для просмотра узлов и объектов кластера, а также для работы с ними служит команда Работа с кластером (WRKCLU). При вызове этой команды показывается окно Работа с кластером. Кроме просмотра узлов и сведений о кластере эту команду можно применить для сбора данных о кластере

| Для сбора сведений для восстановления выполните следующие действия:

| 1. В командной строке введите WRKCLU OPTION (OPTION). С помощью приведенных ниже опций можно указать требуемый тип информации о состоянии.

| *SELECT

| Отображается меню Работа с кластером.

| *CLUINF

| Отображается информация о кластере.

| *CFG Отображаются параметры производительности и конфигурации кластера.

| *NODE

| Отображается панель Работа с узлами кластера, на которой перечислены все узлы кластера.

| *DEVDMN

| Отображается панель Работа с доменами устройств, на которой перечислены все домены устройств кластера.

| *CRG Отображается панель Работа с группами ресурсов кластера, на которой перечислены все группы ресурсов кластера.

| *ADMDMN

| Отображается панель Работа с административными доменами, на которой перечислены все административные домены кластера.

| *SERVICE

| Сбор отладочной информации и данных трассировки для всех заданий служб ресурсов кластера. Эта информация сохраняется в файле. Каждое задание представлено отдельным элементом. Эту опцию рекомендуется применять только по указанию сотрудника службы поддержки. Эта опция вызывает окно с приглашением Создать дамп трассировки кластера (DMPCLUTRC).

| Наиболее частые неполадки кластеров

В этом разделе перечислены наиболее часто встречающиеся неполадки кластеров и обсуждаются способы их предотвращения и устранения их последствий.

В этом разделе перечислены наиболее частые незначительные и легко устранимые неполадки, возникающие при работе с кластерами.

Не удается запустить или перезапустить узел кластера.

Эта неполадка обычно вызвана неправильной настройкой сети. Проверьте, правильно ли заданы сетевые атрибуты: циклический адрес, параметры INETD, атрибут ALWADDCLU и IP-адреса, выделенные кластеру.

- Если ошибка возникает при попытке запустить удаленный узел, следует проверить значение атрибута ALWADDCLU на удаленном узле. Этому атрибуту должно быть присвоено значение *ANY или *RQSAUT, в зависимости от вашей среды.
- IP-адреса, выделенные кластеру на локальном и удаленном узлах, должны находиться в состоянии *Активен*.
- Циклический адрес (127.0.0.1) на локальном и удаленном узлах должен находиться в состоянии 'активен'.
- Локальный и удаленные узлы должны отвечать на запросы PING по IP-адресам, выделенным кластеру.

- На удаленном узле должен быть запущен сервер INETD. Во время работы сервера INETD порт 5550 на удаленном узле должен находиться в состоянии *Прслушивание*. Инструкции по запуску сервера INETD приведены в разделе Сервер INETD.
- До запуска узла на нем должен быть открыт порт 5551.

Удалось создать только несколько разрозненных кластеров, каждый из которых состоит из одного узла.

Такая ситуация чаще всего бывает вызвана проблемами со связью между узлами. Проверьте параметры сети.

Программа выхода работает очень медленно.

Чаще всего эта неполадка бывает вызвана неправильными параметрами в описании задания, используемого программой выхода. Например, может быть указано слишком малое значение параметра MAXACT, из-за чего в каждый момент времени может выполняться слишком мало экземпляров программы выхода. Этому параметру рекомендуется присвоить значение *NOMAX.

В целом наблюдается низкая производительность.

Эта неполадка может быть вызвана целым рядом причин.

- Скорее всего, недостаточна пропускная способность линии связи.
- Еще одна часто встречающаяся причина - несовместимость среды связи и параметров передачи сообщений. Текущие параметры производительности можно посмотреть с помощью API Показать информацию службы ресурсов кластера (QcstRetrieveCRSInfo) и изменить с помощью API Изменить службу ресурсов кластера (QcstChgClusterResourceServices). Параметры производительности кластера, предусмотренные по умолчанию, могут оказаться неэффективными при работе с устаревшими сетевыми адаптерами. В качестве *устаревших* рассматриваются модели 2617, 2618, 2619, 2626 и 2665. Для таких адаптеров следует установить *Класс производительности Обычный*.
- Еще одна возможная причина - неправильная настройка групповой рассылки IP. Если главные адреса кластера (адреса, указанные для узлов при создании кластера или первоначальном добавлении узлов в кластер) находятся в одной локальной сети, в кластере будет применяться функция групповой рассылки пакетов IP. С помощью команды NETSTAT проверьте, определена ли для главных адресов кластера группа рассылки 226.5.5.5. Для этого выберите опцию 14 *Показать группу рассылки*. Если группа рассылки не существует, проверьте, присвоено ли параметру производительности кластера *Применять групповую рассылку* значение ДА. Это можно сделать с помощью API QcstRetrieveCRSInfo (Показать информацию службы ресурсов кластера).
- Если все узлы кластера находятся в одной локальной сети или поддерживают значения MTU, превышающие 1464 байта, то можно значительно повысить производительность за счет увеличения максимального размера сообщений кластера (свыше 1536 Кб) - для этого нужно увеличить значение параметра производительности кластера *Размер фрагмента сообщения* до максимального возможного значения MTU.

Недоступны новые функции, добавленные в текущей версии.

Если при попытке выполнения новой функции появляется сообщение CPFBB70, это означает, что в конфигурации все еще указана предыдущая версия кластера. Нужно установить новую версию кластера на всех узлах, а затем изменить номер версии в конфигурации с помощью интерфейса *Скорректировать версию кластера*. Дополнительная информация приведена в разделе *Коррекция версии кластера*.

Не удалось добавить узел в домен устройств или обратиться к интерфейсу управления кластером Навигатора System i.

Для применения интерфейса управления кластером Навигатора System i и для работы с переносимыми устройствами нужно установить в системе i5/OS компонент 41, - HA Switchable Resources. Для установки этого компонента требуется ключ лицензии.

PTF для кластера установлен, но не работает.

Проверьте, выполнены ли после применения PTF следующие задачи:

1. Завершение работы кластера
2. Выход из системы и повторный вход
До тех пор, пока группа активации не будет уничтожена, в ней будет работать старая версия программы. Весь код кластера (включая API) работает в группе активации, применяемой по умолчанию.
3. Запуск кластера
Большинство PTF кластера требуют для активации завершения и перезапуска узла.

В протоколе программы выхода появляются сообщения CEE0200.

Это сообщение об ошибке выдается процедурой Q_LE_LeBdyPeilog из модуля QLEPM. Все программы, вызываемые программой выхода, должны выполняться в группе активации *CALLER или в явно указанной группе активации. Для устранения этой неполадки нужно скорректировать программу выхода или программу, при вызове которой возникает ошибка.

В протоколе службы ресурсов кластера появляются сообщения CPD000D и CPF0001.

Убедитесь, что системное значение QMLTTHDACN равно 1 или 2.

Кластер не подает признаков жизни.

Проверьте состояние программ выхода CRG. Это можно сделать с помощью команды WRKACTJOB (Работа с активными заданиями): для программ выхода кластера в столбце Функция указано значение PGM-QCSTCRGEXT.

Распад кластера

Большинство неполадок кластера устранить достаточно легко. Распад кластера - это одна из наиболее серьезных неполадок. В этом разделе приведены рекомендации по предотвращению распада кластера и приведен пример процедуры восстановления распавшегося кластера.

Кластер распадается на части в случаях, когда связь между узлами прерывается, но при этом не удается подтвердить выход потерянных узлов из строя. Не следует путать распад кластера с разбиением на логические разделы в среде LPAR.

Если в протоколе хронологии (QHST) или протоколе задания QCSTCTL появится сообщение CPFBB20, оно сигнализирует о распаде кластера и необходимости предпринять действия по устранению последствий распада. Ниже приведен пример распада кластера, состоявшего из четырех узлов: A, B, C и D. В данном примере предполагается, что разорвана связь между узлами B и C, что привело к распаду кластера на две части. Перед распадом кластера существовали четыре CRG (тип CRG не имеет значения): CRG A, CRG B, CRG C и CRG D. В данном примере показаны изменения, которые произошли в доменах восстановления этих CRG в результате распада кластера.

Таблица 35. Пример домена восстановления распавшегося кластера

Узел А	Узел В	х	Узел С	Узел D
CRG A (первый резервный)	CRG A (главный)			
	CRG B (главный)		CRG B (первый резервный)	
	CRG C (главный)		CRG C (первый резервный)	CRG C (второй резервный)
CRG D (второй резервный)	CRG D (главный)		CRG D (первый резервный)	
Часть 1			Часть 2	

Распад кластера может произойти от того, что размер MTU на одном из транзитных участков меньше, чем размер фрагмента сообщения кластера. Значение MTU для IP-адреса кластера можно узнать с помощью команды Работа с состоянием сети TCP/IP (WRKTCPSSTS) на соответствующем узле. Помимо этого, следует проверить значение MTU на всех транзитных участках линии связи. Если MTU меньше, чем размер фрагмента сообщения, нужно либо увеличить MTU, либо уменьшить размер фрагмента сообщения. Текущие параметры производительности можно посмотреть с помощью API Показать информацию службы ресурсов кластера (QcstRetrieveCRSInfo) и изменить с помощью API Изменить службу ресурсов кластера (QcstChgClusterResourceServices).

После устранения причины распада кластер самостоятельно определит, что линия связи вновь работает, и выдаст сообщение CPFBB21 в протокол хронологии (QHST) или в протокол задания QCSTCTL. Это сообщение информирует оператора о том, что распавшийся кластер вновь объединен. Учтите, что на объединение кластера после устранения причин распада может понадобиться несколько минут.

Определение роли частей кластера после распада:

Для того чтобы выполнить правильные действия по устранению последствий распада кластера, нужно определить, какая из частей кластера после распада стала главной, а какие - вторичными. Как только это будет сделано, каждой части кластера будет соответствовать главная или вторичная роль по отношению к группам ресурсов кластера.

В иерархической модели главным будет считаться часть, содержащая текущий главный узел. Все остальные части кластера считаются дополнительными. Для каждой группы ресурсов кластера может быть своя главная часть.

В равноправной модели действуют следующие правила:

- Главной будет считаться та часть, в которую входят все узлы домена восстановления.
- Если узлы домена восстановления входят в несколько частей, то главной среди них не будет. Обе части будут дополнительными.
- Если в какой-либо части кластера нет равноправных узлов и в ней активна группа ресурсов кластера, то работа CRG в этой части будет завершена.
- В дополнительной части разрешены операционные изменения (с учетом их ограничений).
- Изменения конфигурации в дополнительной части не допускаются.

В результате распада устанавливаются следующие ограничения на API для работы с CRG:

Таблица 36. Ограничения на API для работы с CRG, связанные с распадом кластера

API	Разрешено в главной части	Разрешено во вторичных частях
Добавить узел в домен восстановления	X	
Добавить запись устройства в CRG		
Изменить группу ресурсов кластера	X	

Таблица 36. Ограничения на API для работы с CRG, связанные с распадом кластера (продолжение)

API	Разрешено в главной части	Разрешено во вторичных частях
Изменить запись устройства в CRG	X	X
Создать группу ресурсов кластера.		
Удалить группу ресурсов кластера	X	X
Разослать информацию	X	X
Завершить работу CRG ¹	X	
Выполнить принудительный перенос ресурсов	X	
Показать список CRG	X	X
Показать сведения о CRG	X	X
Удалить узел из домена восстановления	X	
Удалить запись устройства из CRG	X	
Запустить CRG ¹	X	
Примечание:		
1. Разрешено для всех частей для CRG, но влияет только на ту часть, в которой запущен API.		

Эти ограничения установлены для того, чтобы сохранить возможность синхронизации CRG после восстановления кластера. По мере того, как узлы будут возвращаться в кластер, CRG с главных узлов будут обновляться на резервных узлах.

При объединении двух дополнительных частей в равноправной модели копироваться на все остальные узлы будет та часть, в которой была активная CRG. Если состояние CRG в обеих частях одинаково, то копироваться будет та часть, в которой был первый узел из списка домена восстановления CRG. Версия CRG в этой части будет копироваться на узлы всех остальных частей.

Как только будет обнаружен распад, во всех частях кластера запрещается применение API Добавить запись узла кластера, Скорректировать версию кластера и Создать кластер. API Добавить запись в домен устройств можно применять только в том случае, если все узлы домена восстановления находятся в одной части кластера. Все API управления кластером можно выполнять без ограничений. Однако действие этих API распространяется только на ту часть кластера, из которой они вызваны.

Перевод узлов после распада кластера в число неисправных:

В некоторых случаях выдается сообщение о разделе кластера, хотя в действительности просто узел вышел из строя. Это происходит в случаях, когда служба теряет связь с некоторыми узлами кластера и не может определить, вышли ли они из строя. Если это требуется, вы можете пометить узлы как сбойные вручную.

Внимание: Если вы пометите узел как сбойный, это упростит восстановление распавшегося кластера. Однако не следует пометить узлы как сбойные в ситуации, когда действительно произошел распад кластера и все узлы по-прежнему работают. В противном случае может возникнуть ситуация, когда несколько узлов в разных частях кластера попытаются выполнять функции главного узла для одной и той же CRG. Это может легко привести к повреждению или рассинхронизации файлов и данных, поскольку все узлы, считающие себя главными узлами CRG, будут независимо друг от друга вносить изменения в собственные копии файлов. Кроме того, если в разных частях кластера находятся узлы, считающие себя главными по отношению к одной и той же CRG, то объединить эти части в кластер невозможно.

Перевод узла в разряд сбойных может повлечь за собой перераспределение ролей в доменах восстановления CRG, в которых участвовал этот узел. Узел, переведенный в разряд сбойных, станет последним резервным узлом. Если несколько узлов вышли из строя одновременно, то итоговый порядок узлов в домене

восстановления будет зависеть от того, в каком порядке эти узлы переводились в разряд сбойных. Если сбойный узел был главным узлом домена восстановления CRG, то первый активный узел в списке резервных станет главным узлом домена восстановления.

Если служба ресурсов кластера потеряет связь с узлом и не сможет определить, работает ли этот узел, то ему будет присвоено состояние **Нет связи**. В некоторых случаях в такой ситуации следует поменять состояние узла с **Нет связи** на **Сбой**. После этого вы сможете перезапустить узел.

Для того чтобы изменить состояние узла с **Нет связи** на **Сбой**, выполните следующие действия:

1. В Web-браузере введите `http://система:2001`, где система - это имя хоста системы.
2. Войдите в систему, указав пользовательский профиль и пароль.
3. Выберите опцию **Службы ресурсов кластеров** в окне Навигатора IBM Systems Director для i5/OS.
4. На странице **Службы ресурсов кластера** выберите задачу **Работа с узлами кластера**, чтобы просмотреть список узлов кластера.
5. Откройте меню **Выбрать действие** и выберите **Изменить состояние**. Укажите, что узел неисправен.

Информация, связанная с данной

Команда Изменить узел кластера (CHGCLUNODE)

API Изменить запись узла кластера (QcstChangeClusterNodeEntry)

Разделенные домены управления кластером:

При работе с разделенными доменами управления кластером необходимо учитывать следующую информацию.

Если домен управления кластером распался, то синхронизация изменений будет продолжаться, но уже среди активных узлов в каждой части. Когда узлы снова объединяются, домен управления кластером собирает все изменения от каждой части и распространяет их, синхронизируя ресурсы по всему домену. Существует несколько замечаний относительно обработки объединения в домене управления кластером:

- Если все части были активными, и в различных частях был изменен один и тот же ресурс, во время объединения для этого ресурса во всех узлах применяется последнее изменение. Самое последнее изменение определяется с использованием Универсального скоординированного времени (UTC) для всех узлов, в которых было инициализировано изменение.
- Если все части были неактивными, глобальные значения для всех ресурсов обрабатываются на основе последнего изменения, внесенного во время активной работы части. Фактические изменения к контролируемым ресурсам не применяются до тех пор, пока не будет запущен равноправный CRG, представляющий домен управления кластером.
- Если перед объединением одни части были активными, а другие - неактивными, глобальные значения, представляющие изменения, внесенные в активных частях, распространяются на неактивные части. Затем неактивные части запускаются, в результате чего все ожидающие изменения, внесенные в узлах неактивных частей, распространяются на объединенный домен.

Советы: распад кластера:

При распаде кластера воспользуйтесь приведенными советами.

1. Ограничения на выполнение операций после распада кластера вводятся для того, чтобы сохранить возможность объединения частей обратно в кластер. Если не соблюдать эти ограничения, то могут быть выполнены операции, после которых восстановление кластера станет чрезвычайно трудоемким.
2. Уничтожение узлов в главной части кластера затрудняет работу с узлами в остальных частях кластера. Обычно потеря узлов главной части кластера происходит из-за физического повреждения помещения, в котором находилась главная часть кластера. Воспользуйтесь примером, приведенным в разделе Устранение ошибок, возникших в результате распада кластера, исходя из предположения, что повреждена часть 1. В этом случае главные узлы для CRG B, C и D будут находиться в части 2. Тогда проще всего восстановить кластер путем перевода узлов A и B в разряд сбойных. Дополнительная

информация об этом приведена в разделе Перевод узлов после распада кластера в разряд сбойных. Кластер можно восстановить вручную. Для этого нужно выполнить следующие действия:

- a. Удалите узлы А и В из кластера для части 2. Теперь часть 2 будет составлять весь кластер.
- b. Настройте в новом кластере среду логической репликации. IE. Воспользуйтесь командой или API Запустить группу ресурсов кластера.

Поскольку из определения кластера в части 2 были удалены узлы, объединение частей 1 и 2 теперь невозможно. Для того чтобы устранить несоответствия в определениях кластера, вызовите API Удалить кластер (QcstDeleteCluster) на всех узлах части 1. Затем добавьте узлы из части 1 в кластер и восстановите все определения CRG, домены восстановления и среду логической репликации. Это требует больших усилий и предельного внимания. Настоятельно не рекомендуется выполнять эту процедуру в случаях, когда можно обойтись менее разрушительными средствами.

3. Процедура запуска узла кластера зависит от состояния запускаемого узла:

Если узел вышел из строя, либо его работа была завершена с помощью операции Завершить работу узла:

- a. На узле, добавляемом в кластер, будет запущена служба ресурсов кластера.
- b. С одного из активных узлов кластера на этот узел будет скопировано определение кластера.
- c. На добавляемый узел будут скопированы определения CRG, в домены восстановления которых входил этот узел. Эти определения будут взяты с других активных узлов кластера. Никакие CRG с добавляемого узла не передаются на другие узлы.

Если узел вышел из кластера в результате распада:

- a. Определение кластера на запускаемом узле сравнивается с определением кластера на одном из активных узлов. Если определения одинаковые, то дальше выполняется обычная процедура объединения кластера. Если определения разные, процедура объединения будет прервана и потребуются вмешательство пользователя.
- b. Если операция объединения будет продолжена, то добавляемый узел станет активным узлом кластера.
- c. Для всех CRG, в домены восстановления которых входит новый активный узел, будет выполнена синхронизация на всех узлах кластера. В ходе синхронизации CRG могут копироваться как на новый активный узел, так и с этого узла на другие.

Прочие неполадки

В этом разделе обсуждаются процедуры восстановления после прочих неполадок в работе кластера.

Устранение последствий сбоев в заданиях кластера:

Аварийное завершение задания службы ресурсов кластера, как правило, свидетельствует о какой-то внешней неполадке.

Просмотрите протокол сбойного задания и найдите сообщения, в которых указана причина сбоя. Устраните причины возникновения ошибки.

Для перезапуска аварийно завершеного задания группы ресурсов кластера, а также для перезапуска поддержки кластера на узле можно воспользоваться командой Изменить восстановление кластера (CHGCLURCY).

1. CHGCLURCY CLUSTER (EXAMPLE) CRG (CRG1) NODE (NODE1) ACTION (*STRCRGJOB) - эта команда вызовет отправку задания группы ресурсов кластера CRG1 на узле NODE1. Для того чтобы на узле NODE1 можно было запустить группу ресурсов кластера, на нем должна быть активна служба ресурсов кластера.
2. Запустите службу ресурсов кластера на узле.

Если вы пользуетесь для работы с кластером продуктом IBM Business Partner, то обратитесь к документации по этому продукту.

Информация, связанная с данной

Команда Изменить восстановление кластера (CHGCLURCY)

Восстановление поврежденного объекта кластера:

Повреждение объектов кластера как таковых маловероятно, но иногда получают повреждения объекты службы ресурсов кластера.

Если система работает в составе кластера, она попытается восстановить поврежденные объекты с другого активного узла. При этом будут выполнены следующие действия:

Если поврежден внутренний объект кластера:

1. Работа узла, на котором поврежден объект, будет завершена.
2. Если в кластере есть еще хотя бы один активный узел, данный узел автоматически перезапустится и вернется в кластер. В процессе возврата узла в кластер поврежденный объект будет исправлен.

Если повреждена CRG:

1. Узел, на котором расположен поврежденный CRG, аварийно завершит все операции, выполняемые в данный момент над этим CRG. После этого система попытается автоматически восстановить поврежденный CRG с другого активного узла кластера.
2. Если в домене восстановления CRG есть еще хотя бы один активный узел, то CRG будет успешно восстановлен. В противном случае задание CRG будет завершено.

Если системе не удастся найти ни одного другого активного узла кластера, то процедуру исправления нужно будет выполнить вручную.

Если поврежден внутренний объект кластера:

Будет выдано сообщение о внутренней ошибке кластера (CPFBB46, CPFBB47 или CPFBB48).

1. Завершите работу службы ресурсов кластера на узле, на котором поврежден объект.
2. Запустите службу ресурсов кластера на этом узле. Данную операцию нужно выполнить с другого активного узла кластера.
3. Если после выполнения шагов 1 и 2 неполадка не будет устранена, удалите узел с поврежденным объектом из кластера.
4. Вновь добавьте этот узел в кластер и в нужные домены восстановления CRG.

Если повреждена CRG:

Будет выдано сообщение о том, что поврежден объект (CPF9804).

1. Завершите работу службы ресурсов кластера на узле, на котором поврежден объект.
2. Удалите CRG с помощью команды DLTCRG.
3. Если в кластере больше нет активных узлов из домена восстановления данного CRG, восстановите CRG из резервной копии.
4. Запустите службу ресурсов кластера на узле, на котором был поврежден объект. Эту операцию можно выполнить с любого активного узла.
5. После запуска службы ресурсов кластера все CRG будут автоматически синхронизированы. Вам может потребоваться вновь создать CRG, если в его домене восстановления нет ни одного узла, кроме данного.

Восстановление кластера после полного выхода из строя:

Информация из этого раздела, а также раздел Восстановление системы помогут вам восстановить систему после полного выхода из строя в результате непредвиденного отключения питания.

Пример 1: Восстановление данных в исходной системе

1. Для предотвращения противоречий в информации о домене устройств LIC и i5/OS рекомендуется установить LIC с помощью опции 3 (Установить LIC и восстановить конфигурацию).

Примечание: Для выполнения этой операции в системе должны быть установлены те же диски, что и на момент сохранения системы. Это требование не распространяется только на загрузочный диск. Кроме того, восстанавливаться должен тот же выпуск операционной системы, который был установлен.

2. После установки Лицензионного внутреннего кода перейдите к процедуре Восстановление конфигурации дисков из раздела *Восстановление системы*. Эта процедура поможет вам обойтись без повторной настройки ASP.
3. После восстановления системы нужно запустить службу ресурсов кластера на локальном узле с другого активного узла. В результате этой операции на узел будет загружена вся информация о кластере.

Пример 2: Восстановление данных в другой системе

После восстановления системы и проверки протокола задания на отсутствие ошибок нужно выполнить следующие действия по настройке домена устройств кластера.

1. С узла, на котором восстановлена система, нужно удалить службу ресурсов кластера.
2. С любого активного узла кластера выполните следующие действия:
 - a. Удалите восстановленный узел из кластера.
 - b. Добавьте восстановленный узел в кластер.
 - c. Добавьте восстановленный узел в домен устройств.
 - d. Создайте CRG или добавьте узел в домен восстановления.

Восстановление кластера после аварии:

Стихийные бедствия могут привести к уничтожению всех узлов кластера, и тогда вам придется полностью восстанавливать кластер.

На случай возникновения такой ситуации рекомендуется сохранить информацию о конфигурации кластера и держать под рукой распечатку этой информации.

Восстановление кластера из резервной копии:

При нормальной работе восстановление с резервной копии обычно не требуется.

Оно необходимо только в случае аварии и потери данных на всех узлах кластера. Если нечто подобное произойдет, то следуйте обычным процедурам восстановления данных из резервной копии.

Устранение неполадок распределенной по сайтам зеркальной защиты

Put your short description here; used for first paragraph and abstract.

Type **your** text here.

- an interesting point
- another interesting point

Subheading

Here's a little section in a concept.

Example

Here's a little example section in a concept.

Сообщения географической зеркальной защиты

Для устранения неполадок географической зеркальной защиты ознакомьтесь с описаниями сообщений географической зеркальной защиты и средствами устранения неполадок.

0x00010259

Описание: Сбой операции. Системе не удалось найти зеркальную копию.

Исправление: Ответили не все узлы домена устройств. Убедитесь, что кластеры запущены. При необходимости запустите кластеры на узле. Дополнительная информация приведена в разделе “Запуск узлов” на стр. 95. Повторите запрос. Если неполадка возникнет снова, обратитесь в сервисный центр.

0x0001025A

Описание: не все пулы дисков в группе пулов дисков используют географическую зеркальную защиту.

Исправление: Если один пул дисков в группе пулов дисков использует географическую зеркальную защиту, то ее должны использовать все пулы дисков в группе пулов дисков. Выполните одно из следующих действий:

1. Настройте географическую зеркальную защиту для пулов дисков, которые не используют географическую зеркальную защиту.
2. Отключите географическую зеркальную защиту для пула дисков, который ее использует.

0x00010265

Описание: Отсоединенная зеркальная копия доступна.

Исправление: Сделайте отсоединенную зеркальную копию недоступной и попробуйте повторить операцию присоединения.

0x00010380

Описание: Дисковый накопитель отсутствует в конфигурации зеркальной копии.

Исправление: Найдите или исправьте отсутствующий диск в зеркальной копии. Проверьте протокол операций продукта на узле получателя. Восстановите кэш-память IOP.

0x00011210

Описание: Указанный вспомогательный пул дисков для группы пулов дисков не использует географическую зеркальную защиту.

Исправление: Если один пул дисков в группе пулов дисков использует географическую зеркальную защиту, то ее должны использовать все пулы дисков в группе пулов дисков. Настройте географическую зеркальную защиту для указанного вспомогательного пула дисков, который ее не использует, сейчас или после завершения этой операции.

0x00011211

Описание: Существуют дубликаты зеркальных копий.

Исправление: Проверьте, существуют ли локальные зеркальные дисковые накопители в обеих системах, Enterprise Storage Server FlashCopy, или копии независимых пулов дисков предыдущих версий. Дополнительную информацию можно найти в протоколе операций продукта на узле зеркальной копии. Устраните дубликат и повторите запрос. Если неполадка возникнет снова, обратитесь в сервисный центр или в техническую поддержку i5/OS для получения подробной информации о поддержке и службах IBM.

Лицензия на исходный код и отказ от обязательств

IBM предоставляет вам неисключительную лицензию на использование всех примеров программного кода. Разрешается создавать на их основе программный код, необходимый вам.

ПРИ УСЛОВИИ СОБЛЮДЕНИЯ ВСЕХ НЕ ДОПУСКАЮЩИХ ИСКЛЮЧЕНИЙ ГАРАНТИЙ, ПРЕДУСМОТРЕННЫХ ЗАКОНОМ, IBM, РАЗРАБОТЧИКИ ПРОГРАММ И ПОСТАВЩИКИ НЕ ПРЕДОСТАВЛЯЮТ КАКИХ-ЛИБО ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ,

НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ, ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ СОБЛЮДЕНИЯ ПРАВ, КОММЕРЧЕСКОЙ ЦЕННОСТИ ИЛИ ПРИМЕНЕНИЯ ДЛЯ КАКИХ-ЛИБО КОНКРЕТНЫХ ЦЕЛЕЙ.

IBM, РАЗРАБОТЧИКИ ПРОГРАММ ИЛИ ПОСТАВЩИК НИ ПРИ КАКИХ УСЛОВИЯХ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА:

1. ПОТЕРЮ ИЛИ ПОВРЕЖДЕНИЕ ДАННЫХ;
2. ПРЯМОЙ, ЧАСТНЫЙ, СВЯЗАННЫЙ ИЛИ КОСВЕННЫЙ УЩЕРБ И ВЫЗВАННЫЙ ИМ ЭКОНОМИЧЕСКИЙ УЩЕРБ; ЛИБО
3. УПУЩЕННУЮ ВЫГОДУ, ПОТЕРЮ КЛИЕНТОВ, ДОХОДОВ, ДЕЛОВОЙ РЕПУТАЦИИ ИЛИ ИСТРАЧЕННЫЕ СБЕРЕЖЕНИЯ.

В НЕКОТОРЫХ ЮРИСДИКЦИЯХ НЕ ДОПУСКАЮТСЯ ИСКЛЮЧЕНИЯ ИЛИ ОГРАНИЧЕНИЯ ПРЯМОГО, СВЯЗАННОГО ИЛИ КОСВЕННОГО УЩЕРБА, ПОЭТОМУ НЕКОТОРЫЕ ИЛИ ВСЕ УКАЗАННЫЕ ВЫШЕ ОГРАНИЧЕНИЯ И ИСКЛЮЧЕНИЯ МОГУТ К ВАМ НЕ ОТНОСИТЬСЯ.

| **Установка лицензионной программы IBM System i High Availability Solutions Manager (iHASM)**

| Перед реализацией решения высокой готовности i5/OS необходимо установить лицензионную программу IBM System i High Availability Solutions Manager (iHASM) (5761-HAS) в каждой системе, включенной в решение высокой готовности.

| Перед установкой лицензионной программы iHASM следует выполнить следующие требования для установки:

- | 1. Установите или обновите систему до V6R1 i5/OS.
- | 2. Установите Опцию 41 i5/OS (Переносимые ресурсы HA).

| Для установки лицензионной программы iHASM выполните следующие действия:

- | 1. В командной строке введите GO LICPGM.
- | 2. В меню Работа с лицензионными программами выберите опцию 11 (Установить лицензионные программы).
- | 3. Выберите Компонент 5761-HAS, опцию *BASE для установки iHASM для System i. Нажмите Enter.
- | 4. В меню Опции установки введите имя требуемого установочного устройства. Для начала установки нажмите Enter.

Приложение. Примечания

Настоящая документация была разработана для продуктов и услуг, предлагаемых на территории США.

IBM может не предлагать продукты и услуги, упомянутые в этом документе, в других странах. Информацию о продуктах и услугах, предлагаемых в вашей стране, вы можете получить в местном представительстве IBM. Ссылка на продукт, программу или услугу IBM не означает, что может применяться только этот продукт, программа или услуга IBM. Вместо них можно использовать любые другие функционально эквивалентные продукты, программы или услуги, не нарушающие прав IBM на интеллектуальную собственность. Однако в этом случае ответственность за проверку работы этих продуктов, программ и услуг возлагается на пользователя.

Продукты и технологии, описанные в документе, могут быть запатентованы IBM. Предоставление настоящего документа не означает предоставления каких-либо лицензий на патенты. Запросы на приобретение лицензий можно отправлять по следующему адресу:

IBM
Director of Licensing
IBM Corporation North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Запросы на лицензии, связанные с информацией DBCS, следует направлять в отдел интеллектуальной собственности в местном представительстве IBM или (в письменном виде) по следующему адресу:

IBM World Trade Asia Corporation
Лицензирование
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Следующий абзац не относится к Великобритании, а также другим странам, в которых это заявление противоречит местному законодательству: ФИРМА INTERNATIONAL BUSINESS MACHINES CORPORATION ПРЕДОСТАВЛЯЕТ НАСТОЯЩУЮ ПУБЛИКАЦИЮ НА УСЛОВИЯХ “КАК ЕСТЬ”, БЕЗ КАКИХ-ЛИБО ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ, НЕЯВНЫЕ ГАРАНТИИ СОБЛЮДЕНИЯ ПРАВ, КОММЕРЧЕСКОЙ ЦЕННОСТИ И ПРИГОДНОСТИ ДЛЯ КАКОЙ-ЛИБО ЦЕЛИ. В некоторых странах запрещается отрицать предоставление каких-либо явных и подразумеваемых гарантий при заключении определенных договоров, поэтому указанное заявление может не иметь места в вашем случае.

В данной публикации могут содержаться технические неточности и типографские опечатки. В информацию периодически вносятся изменения, которые будут учтены в последующих изданиях настоящей публикации. IBM оставляет за собой право в любое время и без дополнительного уведомления исправлять и обновлять продукты и программы, упоминаемые в настоящей публикации.

Все ссылки на информацию, приведенную на Web-сайтах других фирм, приведены только для удобства. Фирма IBM не гарантирует достоверность этой информации. Материалы, размещенные на этих Web-сайтах, не являются частью документации по данному продукту IBM, и ответственность за применение этих материалов лежит на пользователе.

IBM может использовать и распространять любую предоставленную вами информацию на свое усмотрение без каких-либо обязательств перед вами.

Для получения информации об этой программе для обеспечения: (i) обмена информацией между независимо созданными программами и другими программами (включая данную) и (ii) взаимного использования информации, полученной в ходе обмена, пользователи данной программы могут обращаться по адресу:

IBM Corporation Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N Rochester, MN 55901
U.S.A.

Такая информация может предоставляться на определенных условиях, включая, в некоторых случаях, уплату вознаграждения.

| Описанная в этом документе лицензионная программа и все связанные с ней лицензионные материалы
| предоставляются IBM в соответствии с условиями Соглашения с заказчиком IBM, Международного
| соглашения о лицензии на программу IBM, Лицензионного соглашения о машинном коде IBM или любого
| другого эквивалентного соглашения.

Данные о быстродействии, приведенные в документах, были получены на системах, настроенных особым образом. Результаты, полученные в других средах, могут существенно отличаться от приведенных. Некоторые измерения могли быть выполнены в системах, находящихся на этапе разработки, поэтому результаты измерений, полученные в серийных системах, могут отличаться от приведенных. Более того, результаты некоторых измерений могли быть получены в результате экстраполяции. Фактические результаты могут различаться. Систему следует настроить в соответствии с рекомендациями, приведенными в документе.

Информация о продуктах других фирм была получена от поставщиков этих продуктов, из опубликованных ими документов или других общедоступных источников. Эти продукты не были проверены IBM. Точность приводимых данных о быстродействии, совместимости и других сведений о продуктах, выпущенных сторонними компаниями, не гарантируется. Запросы на получение дополнительной информации об этих продуктах должны направляться их поставщикам.

Все заявления о будущих намерениях и планах фирмы IBM приведены только для общего сведения. Фирма IBM оставляет за собой право отказываться от этих заявлений и вносить в них изменения без дополнительного предупреждения.

Все приведенные цены IBM являются текущими рекомендованными розничными ценами IBM и могут быть изменены без предварительного уведомления. Цены дилеров могут быть другими.

Данная информация носит предварительный характер и предназначена только для планирования. Информация может измениться до того, как описанные в ней продукты станут доступными.

Эта информация содержит примеры данных и отчетов, применяемых в повседневной работе. Для максимальной достоверности в них приведены имена отдельных лиц, названия компаний, товарных знаков и продуктов. Все эти имена и названия вымышлены, и любое их сходство с реальными именами, названиями и адресами носит совершенно случайный характер.

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ:

Данная документация содержит примеры исходного текста программы, иллюстрирующие различные приемы программирования для различных платформ. Вы можете копировать, видоизменять и распространять эти примеры программ в любом виде без возникновения каких-либо денежных обязательств перед IBM с целью разработки, применения, продажи или распространения прикладных программ, соответствующих стандартам интерфейсов прикладного программирования для той платформы, для которой написаны эти примеры программ. Работа примеров не была проверена во всех возможных условиях. Поэтому IBM не может гарантировать или подразумевать надежность, пригодность и функциональность этих программ.

Каждая полная или частичная копия, а также программа, включающая такую копию, должна содержать следующую информацию об авторских правах:

© (название вашей компании) (год). Этот код разработан на основе примеров кода фирмы IBM © Copyright IBM Corp. _год или годы_. Все авторские права сохранены.

Если данный документ представлен в электронном виде, в нем могут отсутствовать фотографии и цветные иллюстрации.

Информация об интерфейсе программирования

В настоящей документации приведена информация об интерфейсах программирования панели управления, позволяющих заказчикам создавать программы, использующие службы IBM i5/OS.

Товарные знаки

Ниже перечислены товарные знаки фирмы International Business Machines Corporation, зарегистрированные в США и/или других странах:

i5/OS
IBM
IBM (эмблема)
System i
System i5
IBM Systems Storage
TotalStorage
FlashCopy

- | Adobe, эмблема Adobe, PostScript и эмблема PostScript являются товарными знаками или зарегистрированными товарными знаками Adobe Systems Incorporated в США и/или других странах.
- | Microsoft, Windows, Windows NT и эмблема Windows являются товарными знаками корпорации Microsoft в США и/или других странах.
- | Java и все товарные знаки на основе Java являются товарными знаками Sun Microsystems, Inc. в США и/или других странах.

Другие названия фирм, продуктов и услуг могут являться товарными знаками или знаками обслуживания других фирм.

Условия и соглашения

Разрешение на использование этих публикаций предоставляется в соответствии с следующими условиями и соглашениями.

Личное использование: Вы можете воспроизводить эти публикации для личного, некоммерческого использования при условии сохранения информации об авторских правах. Данные публикации, а также любую их часть запрещается распространять, демонстрировать или использовать для создания других продуктов без явного согласия IBM.

Коммерческое использование: Вы можете воспроизводить, распространять и демонстрировать эти публикации в рамках своей организации при условии сохранения информации об авторских правах. Данные публикации, а также любую их часть запрещается воспроизводить, распространять, использовать для создания других продуктов и демонстрировать вне вашей организации, без явного согласия IBM.

На данные публикации, а также на содержащиеся в них сведения, данные, программное обеспечение и другую интеллектуальную собственность, не распространяются никакие другие разрешения, лицензии и права, как явные, так и подразумеваемые, кроме оговоренных в настоящем документе.

IBM сохраняет за собой право аннулировать предоставленные настоящим документом разрешения в том случае, если по мнению IBM использование этих публикаций может принести ущерб интересам IBM или если IBM будет установлено, что приведенные выше инструкции не соблюдаются.

Вы можете загружать, экспортировать и реэкспортировать эту информацию только в полном соответствии со всеми применимыми законами и правилами, включая все законы США в отношении экспорта.

IBM не несет ответственности за содержание этих публикаций. Публикации предоставляются на условиях "как есть", без предоставления каких-либо явных или подразумеваемых гарантий, включая, но не ограничиваясь этим, подразумеваемые гарантии коммерческой ценности, отсутствия нарушений или применения для каких-либо конкретных целей.



Напечатано в Дании