ТЕМА 6. ОРГАНИЗАЦИЯ ХРАНЕНИЯ ДАННЫХ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

В данной теме рассматриваются следующие вопросы:

- технологии хранения данных: DAS, NAS, SAN;
- виды SAN;
- реализация iSCSI в операционных системах семейства Windows;
- реализация Storage Spaces;
- предоставление общего доступа к файловым ресурсам;
- служба File Server Resource Manager, файловые квоты и скрининг;
- пространства имен DFS и репликация DFS;
- организация хранения документов с помощью Microsoft SharePoint Server;
- физические и логические компоненты фермы SharePoint;
- иерархия объектов SharePoint;
- типы содержимого, теги и ключевые слова;
- веб-приложения и коллекции сайтов;
- списки и библиотеки SharePoint.

Лекции – 4 часа, лабораторные занятия – 4 часа, самостоятельная работа – 12 часов.

Минимальный набор знаний:

Сравнение DAS, NAS и SAN

Подключение к iSCSI-target

Общие папки: UNC-путь, скрытые папки, ABE

Два вида пространств имен DFS

FSRM: квоты на папки, фильтрация файлов, классификация файлов

6.1. Доступ к данным в локальных файловых системах

Хранение данных — это ключевой компонент, который вы должны учитывать при планировании и развертывании инфраструктуры центра обработки данных. Большинство организаций требуют больших объемов хранения, и это требование всегда увеличивается. Пользователи регулярно работают с приложениями, которые создают новые файлы, которые требуют хранения в центральном месте. Когда пользователи сохраняют свои файлы в течение более длительного времени, требования к хранилищу возрастают.

За последние несколько лет возможности хранения значительно расширились, с внедрением новых технологий и расширением существующих. Поэтому, планируя решения для хранения данных, вы должны учитывать технологии вашей текущей среды и влияние внедрения новых технологий. Многие организации стандартизировали основную группу поставщиков аппаратных средств и стандартов связи, а виртуализация побуждает многих администраторов переоценивать эти стандарты и приступить к размышлениям о решениях хранения следующего поколения для сильно виртуализированных инфраструктур. Этот пункт описывает вам различные аппаратные средства хранения и коммуникационные технологии.

6.1.1. Технологии хранения данных

Когда вы планируете хранение данных, вам нужно определить, как ваши серверы будут обращаться к дискам. В некоторых случаях вы можете подключать диски непосредственно к серверам, которым требуется хранилище (DAS). Однако на предприятиях обычно данные хранятся в NAS или SAN, что обеспечивает большую гибкость. В этом подпункте вы узнаете о различных методах, которые вы можете использовать для предоставления серверам доступа к хранилищу.

6.1.1.1. Хранилище с непосредственным подключением (DAS)

Почти все серверы предоставляют встроенное хранилище или хранилище с непосредственным подключением (Direct-Attached Storage, DAS). DAS может включать в себя диски, которые физически расположены внутри сервера или которые напрямую подключаются к внешнему массиву, или диски, которые подключаются к серверу с помощью USB-кабеля или альтернативного разъема. Однако, поскольку вы подключаете хранилище DAS к серверу физически, хранилище становится недоступно, когда сервер выходит из строя. DAS поставляется с различными типами дисков, такими, как Serial ATA (SATA), последовательный подключенный SCSI (Serial Attached SCSI, SAS) или твердотельный накопитель (Solid-State Drive, SSD). Все эти типы дисков предлагают разные уровни производительности и имеют преимущества и недостатки.

Преимущества использования DAS

Типичная система DAS имеет устройство хранения данных, которое включает в себя несколько жестких дисков, которые подключаются непосредственно к компьютеру через адаптер главной шины (HBA). Нет никаких промежуточных сетевых устройств — концентраторов, коммутаторов или маршрутизаторов —

между DAS и компьютером, но хранилище напрямую подключается к серверу, который его использует. Поэтому DAS — это самая простая система хранения для развертывания и обслуживания.

DAS, как правило, является наименее дорогостоящим хранилищем, которое доступно, и оно доступно широко в различных вариантах скорости и емкости для размещения различных установок. Кроме того, это недорого и очень легко настроить. В большинстве случаев достаточно просто подключить устройство, убедиться, что операционная система Windows его распознает, а затем использовать функцию управления дисками для настройки дисков.

Недостатки использования DAS

Хранение данных локально в DAS затрудняет централизацию данных, поскольку данные находятся на нескольких серверах. Это может усложнить резервное копирование данных, и пользователям может оказаться труднее найти нужные данные. Кроме того, если какое-либо устройство, к которому подключено DAS, испытывает перебои в подаче электроэнергии, хранилище на этом устройстве также становится недоступным.

При использовании DAS выделение дополнительного дискового пространства для серверов может быть более сложным, чем при использовании SAN. С DAS физический диск должен быть установлен на сервере, тогда как при использовании SAN имеющееся нераспределенное пространство может быть предоставлено серверу за несколько щелчков мыши, без физического доступа к серверу.

6.1.1.2. Хранилище с подключением по сети (NAS)

NAS (Network Attached Storage) — это выделенное устройство хранения, доступ к которому осуществляется по сети. NAS отличается от DAS тем, что хранилище не подключается напрямую к каждому отдельному серверу, а скорее доступно через сеть для многих серверов. NAS имеет два отличных решения: низкопроизводительное устройство (NAS only) и NAS предприятия, которое интегрируется с SAN.

Каждое устройство NAS имеет специальную операционную систему, которая полностью контролирует доступ к данным на этом устройстве, что уменьшает накладные расходы, связанные с совместным использованием устройства хранения с другими серверными службами. Windows Storage Server, функция Windows Server 2016, является примером программного обеспечения NAS.

Обычно устройства NAS обеспечивают доступ к хранилищу на уровне файлов, что означает, что данные в хранилище доступны только в виде файлов и папок, и вы должны использовать такие протоколы, как Common Internet File System (CIFS), Server Message Block (SMB) или Network File System (NFS) для доступа к файлам.

Устройства хранения NAS обычно не имеют каких-либо компьютерных интерфейсов, таких как клавиатуры, мыши и мониторы. Чтобы настроить устройство, вам необходимо задать сетевую конфигурацию, а затем получить доступ к устройству по сети. Затем вы можете создавать общие папки на устройстве. Эти общие папки затем доступны пользователям сети.

Преимущества использования NAS

NAS — идеальный выбор для организаций, которые ищут простой и экономичный способ быстрого доступа к данным на уровне файлов для нескольких клиентов. Пользователи NAS выигрывают от повышения производительности и производительности, поскольку вычислительная мощность устройства NAS предназначена исключительно для распределения файлов.

NAS также хорошо вписывается в рынок как решение средней цены. Это не дорого, но он удовлетворяет больше потребностей, чем DAS, следующими способами:

• ёмкость хранилища NAS обычно намного больше, чем DAS;

• NAS обычно использует технологии RAID для избыточности данных;

• NAS обеспечивает единое местоположение для всех критических файлов, а не размещает их на разных серверах с помощью DAS;

• NAS предлагает централизованное хранилище по доступной цене;

• разделы NAS доступны из любой операционной системы, они часто поддерживают несколько протоколов и могут одновременно обслуживать данные через CIFS и NFS. Например, хосты Windows и Linux могут одновременно обращаться к разделу NAS.

Недостатки использования NAS

NAS работает медленнее, чем технологии SAN. Вы обычно обращаетесь к NAS с помощью протоколов Ethernet, и он в значительной степени зависит от сети, поддерживающей решение NAS. Поэтому NAS обычно используется в качестве решения для совместного использования файлов и хранения, но вы не можете (и не должны пытаться) использовать его с такими интенсивными данными программами, интенсивно работающими с дисками, например, с Microsoft Exchange Server и Microsoft SQL Server.

NAS является доступным для предприятий малого и среднего бизнеса, но обеспечивает меньшую производительность и может быть менее надежным, чем SAN. По этой причине большинство крупных предприятий используют SAN, а не NAS.

6.1.1.3. Сети хранения данных (SAN)

Третий тип хранения — это SAN (Storage Area Network), которая является высокоскоростной сетью, которая соединяет компьютерные системы или хост-серверы с высокопроизводительными подсистемами хранения. SAN обычно включает в себя различные компоненты, такие как HBA (Host Bus Adapter), специальные коммутаторы, которые помогают маршрутизировать трафик, и дисковые массивы, на которых создаются LUN (Logical Unit Number) для хранения данных.

SAN позволяет нескольким серверам получить доступ к системе хранения данных, в котором любой сервер может получить доступ к любому LUN. Однако, поскольку SAN использует сеть, вы можете использовать ее для подключения многих разных устройств и хостов и для обеспечения доступа к любому подключенному устройству практически из любого места.

SAN обеспечивают доступ на уровне блоков. Это означает, что вместо того, чтобы использовать протокол доступа к файлу для доступа к содержимому диска в виде файлов, SAN записывают блоки данных непосредственно на диски с помощью таких протоколов, как Fibre Channel, Fibre Channel over Ethernet или Internet SCSI (iSCSI).

Сегодня большинство решений SAN предлагают SAN и NAS вместе. Бэкэнд-головные устройства, диски и технологии идентичны, и метод доступа — это единственное, что меняется. Предприятия часто подключают блочное хранилище SAN к серверам с использованием Fibre Channel over Ethernet или iSCSI, тогда как службы NAS обычно доступны через CIFS и NFS.

Преимущества использования SAN

Технологии SAN читают и записывают на блочном уровне, что значительно ускоряет доступ к данным. Например, при использовании большинства решений DAS и NAS, если вы пишете файл объемом 8 гигабайт (ГБ), весь файл должен быть прочитан/записан и подсчитана его контрольная сумма. Однако с SAN файл записывается на диск в зависимости от размера блока, для которого вы настраиваете SAN. Эта скорость достигается за счет использования Fibre Channel и записи на уровне блоков вместо чтения/записи всего файла с помощью контрольной суммы.

SAN также обеспечивают:

- **Централизацию хранилища в единый пул,** который позволяет ресурсам хранения и ресурсам сервера изменяться независимо. При необходимости они также включают динамическое назначение дискового пространства из пула. Вы можете увеличить или уменьшить хранилище на заданном сервере по мере необходимости, без сложной реконфигурации или переустановки устройств.
- **Общую инфраструктуру для хранения хранилища**, которая позволяет использовать одну общую модель управления для конфигурации и развертывания.
- **Устройства хранения**, которые несколько систем могут использовать естественно, как обычные диски;
- **Передачу данных** непосредственно с устройства на устройство без вмешательства сервера.
- **Высокий уровень избыточности**. Вы развертываете большинство сетей SAN через сеть с несколькими сетевыми устройствами и путями. Кроме того, устройство хранения содержит резервные компоненты, такие как источники питания и жесткие диски.

Недостатки использования SAN

Основным недостатком технологии SAN является то, что вам, вероятно, понадобятся инструменты управления и специальные навыки, связанные с конфигурацией. Кроме того, она значительно дороже, чем DAS или NAS. SAN начального уровня без дисков часто стоит столько же, сколько полностью сконфигурированный сервер с DAS или NAS-устройством.

Чтобы управлять SAN, вы должны хорошо понимать базовую технологию, включая настройку LUN, сети Fibre Channel, размер блока и других факторов.

Кроме того, каждый поставщик систем хранения данных часто реализует SAN с помощью собственных, уникальных инструментов и функций. Поэтому организации часто выделяют специалистов для обслуживания исключительно SAN.

6.1.1.4. Сравнение блочных и файловых устройств хранения данных

Вы можете хранить данные на диске двумя способами: на уровне блоков и на уровне файлов. Часто одна или другая схема является лучшим решением в конкретном сценарии. Однако иногда они дополняют друг друга в инфраструктуре хранения. Например, обычно используется оба типа хранилищ в крупных корпоративных средах.

Хранилище на уровне блоков обычно используется в сочетании с SAN, а хранилище на уровне файлов в сочетании с NAS, Кроме того, хранилище на уровне файлов физически обычно размещается на блочном устройстве хранения.

Хранилище на уровне блоков

Хранилище на уровне блоков подключается к серверам через SAN, чаще всего с использованием одного из протоколов связи SAN, таких как iSCSI, Fibre Channel или Fibre Channel over Ethernet. Администраторы хранилищ создают тома хранилища из отдельных фрагментов дискового пространства блочного хранилища. Внутри томов администраторы хранилища создают LUN, которые являются виртуальными областями хранения. Далее LUN настраивают и публикуют для использования на одном или нескольких серверах.

Серверы видят опубликованные LUN как физические жесткие диски, а администраторы создают тома в Windows Server 2016 на основе LUN. Тома отформатированы в файловой системе, такой как файловая система NTFS или Resilient File System (ReFS), а затем доступны так же, как физический или виртуальный жесткий диск.

Хранилище на уровне блоков имеет следующие характеристики:

- Оно очень гибкое. Например, вы можете использовать его в качестве тома операционной системы, тома данных или хранилища для общих папок.
- Оно не привязан к конкретной операционной системе или конкретной файловой системе. Поддержка всех основных операционных систем и файловых систем.
- Операционные системы могут загружаться с LUN на уровне блоков. Это означает, что ваша организация может развертывать бездисковые физические серверы. В таком сценарии серверы используют Fibre Channel или iSCSI HBA для подключения к их загрузочному LUN при запуске.
- Вы можете подключить хранилище на уровне блоков непосредственно к виртуальным машинам для удовлетворения потребностей в высокопроизводительных хранилищах. В Hyper-V вы можете представить хранилище на уровне блоков для виртуальных машин с помощью сквозного диска (pass-through disk) или с помощью виртуального Fibre Channel.

Хранилище файлового уровня

CIFS и NFS являются основными протоколами связи, которые использует хранилище на уровне файлов. Первоначально CIFS была расширенной версией SMB. Однако сегодня термины CIFS и SMB часто используются взаимозаменяемо.

Microsoft продолжает совершенствовать CIFS со многими основными выпусками операционной системы Windows Server. Хранилище файлового уровня имеет следующие характеристики:

- Доступ к хранилищу на уровне файлов происходит только через протоколы обмена файлами.
- Файловое хранилище находится поверх хранилища на уровне блоков и имеет файловую систему.
- Некоторые приложения поддерживают хранение данных на уровне файлов, а другие — нет. В Windows Server 2012 R2 Hyper-V начал поддерживать хранилище виртуальных машин в общих папках SMB 3.0.
- Хранилище файлового уровня часто более экономично, чем хранение на уровне блоков.

6.1.2. Реализация iSCSI в операционных системах семейства Windows

Служба сервера iSCSI Target (iSCSI Target Server Service) в Windows Server 2012 позволяет серверу Windows реализовать хранилище данных iSCSI, а клиентам (инициаторам) iSCSI — монтировать это хранилище как локальные диски. Доступ к хранилищу iSCSI возможен через Ethernet, и при подключении хранилищу iSCSI можно назначить букву диска и использовать как обычное локальное хранилище. Многие приложения на сервере могут пользоваться хранилищем iSCSI, но перед развертыванием любого приложении в хранилище iSCSI обязательно проверьте системные требования этого приложения.

iSCSI (Internet Small Computer System Interface) — это протокол, который базируется на TCP/IP и разработан для установления взаимодействия и управления системами хранения данных, серверами и клиентами.

iSCSI описывает:

- транспортный протокол для SCSI, который работает поверх TCP;
- новый механизм инкапсуляции SCSI команд в IP сети;
- протокол для новой генерации систем хранения данных, которые будут использовать «родной» TCP/IP

Архитектура обычного SCSI базируется на клиент-серверной модели. Клиент, например, сервер или рабочая станция, инициирует запросы на считывание или запись данных с исполнителя — сервера, например, системы хранения данных. Команды, которые выдает клиент и обрабатывает сервер помещаются в Command Descriptor Block (CDB). Сервер выполняет команду, а окончание ее выполнения обозначается специальным сигналом. Инкапсуляция и надежная доставка CDB транзакций между инициаторами и исполнителями через TCP/IP сеть и есть главная задача iSCSI, причем ее приходится осуществлять в нетрадиционной для SCSI, потенциально ненадежной среде IP сетей.

На рис. 6.1 показана модель уровней протокола iSCSI, которая дает возможность понять порядок инкапсуляции SCSI команд для передачи их через физический носитель.

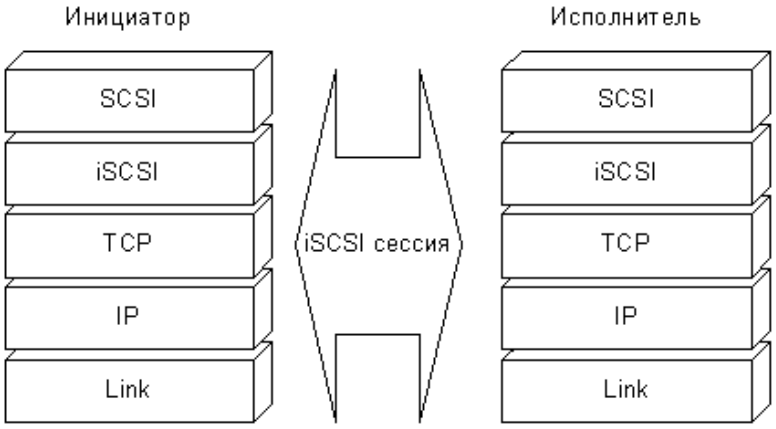

Рис. 6.1. Модель нижних уровней протокола iSCSI

iSCSI-протокол осуществляет контроль передачи блоков данных и обеспечивает подтверждение достоверности завершения операции ввода/вывода. Что, в свою очередь, обеспечивается через одно или несколько TCP соединений.

iSCSI имеет четыре составляющие:

- управление именами и адресами (iSCSI Address and Naming Conventions);
- управление сеансом (iSCSI Session Management);
- обработка ошибок (iSCSI Error Handling);
- безопасность (iSCSI Security).

Управление именами и адресами

Так как iSCSI-устройства являются участниками IP-сети, они имеют индивидуальные Сетевые Сущности (Network Entity). Сетевая Сущность может содержать один или несколько iSCSI-узлов (рис. 6.2).

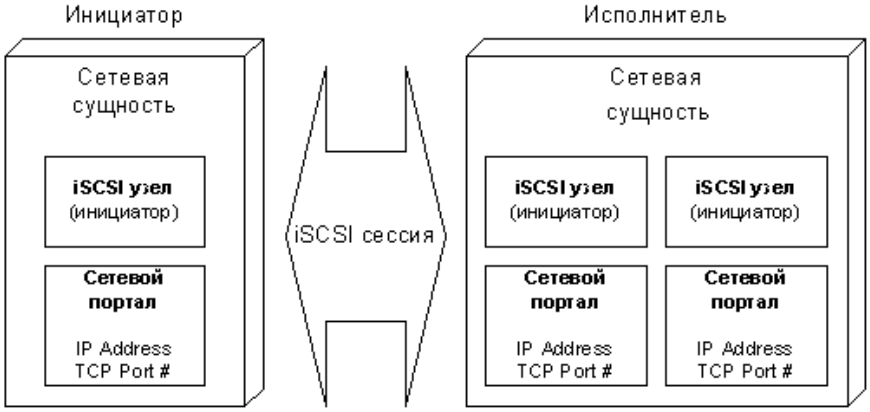

Рис. 6.2. Модель сетевых сущностей

iSCSI-узел является идентификатором SCSI-устройств (в Сетевой Сущности), доступных через сеть. Каждый iSCSI-узел имеет уникальное iSCSI-имя (длиной до 255 байт), которое формируется по правилам, принятым для обозначения узлов в Internet. Например, fqn.by.storage.disksta.777. Такое название имеет удобную для восприятия человеком форму и может обрабатываться DNS-сервером. Таким образом, iSCSI-имя обеспечивает корректную идентификацию iSCSI-устройства вне зависимости от его физического местонахождения. В то же время, в процессе контроля и передачи данных между устройствами удобнее пользоваться комбинацией IP-адреса и TCP-порта, которые обеспечиваются Сетевым порталом (Network Portal). iSCSI-протокол дополнительно к iSCSI-

именам обеспечивает поддержку псевдонимов, которые, как правило, отображаются в системах администрирования для удобства идентификации и управления администраторами системы.

Управление сеансом

iSCSI-сессия состоит из фазы аутентификации (Login Phase) и фазы обмена (Full Feature Phase), которая завершается специальной командой.

Фаза аутентификации iSCSI аналогична процессу Fibre Channel Port Login (PLOGI). Она используется для того, чтобы согласовать разнообразные параметры между двумя Сетевыми Сущностями и подтвердить право доступа инициатора. Если фаза аутентификации iSCSI завершается успешно, исполнитель подтверждает login-инициатору, иначе логин не подтверждается, а TCP-соединение закрывается.

Как только login подтвердится, iSCSI-сессия переходит к фазе обмена. Если было установлено более одного соединения TCP, iSCSI требует, чтобы каждая пара команда/ответ проходила через одно TCP соединение. Такая процедура гарантирует, что каждая отдельная команда считывания или записи будет осуществляться без необходимости дополнительно отслеживать каждый запрос по поводу его прохождения по разным потокам. Однако разные транзакции могут одновременно передаваться через разные TCP соединения в рамках одной сессии (рис. 6.3).

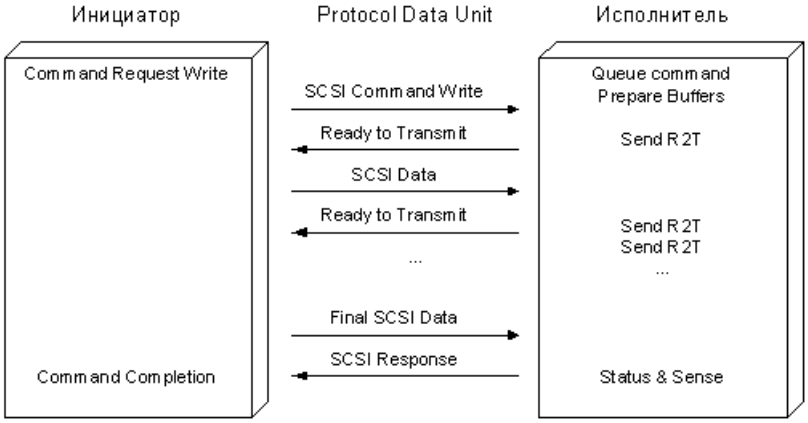

Рис 6.3. Пример iSCSI Write

В завершение транзакции инициатор передает/принимает последние данные, а исполнитель отправляет ответ, который подтверждает успешную передачу данных.

В случае необходимости закрыть сессию, используется команда iSCSI logout, которая передает информацию о причинах завершения сессии. Она также может передать информацию о том, какое соединение следует закрыть в случае возникновения ошибки соединения, чтобы закрыть проблемные TCP-связи.

Обработка ошибок

В связи с высокой вероятностью возникновения ошибок при передаче данных в некоторых типах IP-сетей, в особенности WAN реализациях, в которых может функционировать iSCSI, протокол предусматривает массу мероприятий по обработке ошибок.

Для того, чтобы обработка ошибок и восстановление после сбоев функционировали корректно, как инициатор, так и исполнитель должны иметь возможность буферизации команд до момента их подтверждения. Каждое конечное устройство должно иметь возможность выборочно восстановить утраченный или испорченный PDU в рамках транзакции для восстановления передачи данных.

Иерархия системы обработки ошибок и восстановление после сбоев в iSCSI включает:

На наиболее низком уровне — определение ошибки и восстановление данных на уровне SCSI задачи, например, повторение передачи утраченного или поврежденного PDU.

На следующем уровне — в TCP соединении, которое передает SCSI задачу, может произойти ошибка, а именно, TCP соединение может повредиться. В этом случае осуществляется попытка восстановить соединение.

И, наконец, сама iSCSI-сессия может испортиться. Терминация и восстановление сессии, как правило, не требуется, если восстановление корректно отрабатывается на других уровнях, однако может произойти обратное. Такая ситуация требует закрытия всех TCP соединений, завершения всех задач, недовыполненных SCSI команд и перезапуска сессии через повторный login.

Безопасность

В связи с использованием iSCSI в сетях, где возможен несанкционированный доступ к данным, спецификация предусматривает возможность использования разнообразных методов для повышения безопасности. Такие средства шифрования, как IPSec, которые используют нижние уровни, не требуют дополнительного согласования, так как являются прозрачными для верхних уровней, в том числе для iSCSI. Для аутентификации могут использоваться разнообразные решения, например, такие, как Kerberos, или обмен Частными Ключами, в качестве репозитария ключей может использоваться iSNS-сервер.

6.1.3. Другие сетевые технологии хранения данных

В рамках работы над сетевыми технологиями хранения данных в Internet Engineering Task Force (IETF) была создана рабочая группа IP Storage (IPS) по направлениям:

iSCSI (Internet Small Computer Systems Interface);

FCIP (Fibre Channel over TCP/IP);

iFCP (Internet Fibre Channel Protocol);

iSNS (Internet Storage Name Service).

Fibre Channel over IP

Наименее революционным из трех названых выше является протокол Fibre Channel over IP. Он не вносит значительных изменений в структуру SAN и в организацию самых систем хранения данных. Главная идея этого протокола — реализация возможности объединения географически отдаленных сетей хранения данных.

На рис. 6.4 показан стек протокола FCIP.

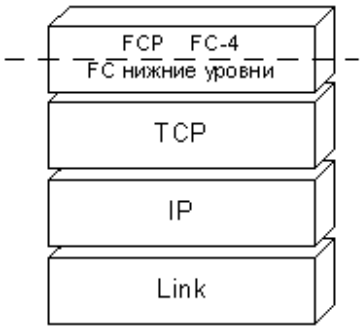

Рис. 6.4. Нижние уровни протокола FCIP

FCIP помогает эффективно решить задачу территориального распределения, и объединения SAN на больших расстояниях. Его основными преимуществами является то, что этот протокол полностью прозрачен для существующих FC SAN сетей и ориентирован на использование инфраструктуры современных MAN/WAN сетей. Таким образом, для обеспечения новой функциональности пользователям, которые ищут возможности связать между собою географически отдаленные FC SAN, будет нужен всего лишь FCIP-шлюз и подключение к MAN/WAN сети. Географически распределенная SAN, построенная с помощью FCIP, воспринимается SAN устройствами как обычная FC сеть, а для MAN/WAN сети, к которой она подключена, она представляет обычный IP трафик.

iFCP

Internet Fibre Channel Protocol — это протокол, который обеспечивает передачу FC-трафика поверх TCP/IP-транспорта между шлюзами iFCP. В этом протоколе транспортный уровень FC замещается транспортом IP-сети, трафик между FC-устройствами маршрутизируется и коммутируется средствами TCP/IP. Протокол iFCP предоставляет возможность подключать существующие FC-системы хранения данных к IP-сети с поддержкой сетевых сервисов, которые нужны этим устройствам.

Стек протокола iFCP показан на рис.6.5:

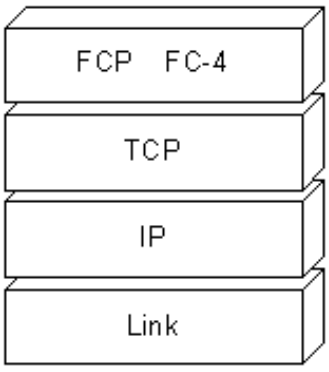

Рис. 6 5. Нижние уровни протокола iFCP

iFCP, согласно спецификации:

- накладывает кадры FC для их транспортирования на предварительно определенное TCP соединение;
- FC сервисы передачи сообщений и маршрутизации перекрываются в шлюзовом устройстве iFCP, таким образом, сетевые структуры и компоненты FC не сливаются в общую FC SAN, а управляются средствами TCP/IP;

- динамично создает IP туннели для FC кадров.

Важной особенностью iFCP является то, что этот протокол обеспечивает FC device-to-device связь (связь между устройствами) через IP-сеть, которая является значительно более гибкой схемой, если сравнивать ее со связью SAN-to-SAN. Так, например, если iFCP имеет TCP-связь между парами портов N_Port двух FC устройств, такая связь может иметь свой собственный уровень QoS, который будет отличаться от уровня QoS другой пары FC устройств.

6.2. Сетевой доступ к файловым ресурсам

6.2.1. Предоставление общего доступа к файловым ресурсам

Это традиционный и наиболее часто применяемый метод для доступа к данным сервера с помощью протокола SMB (Server Message Block - блок сообщений сервера) через TCP /IP. Системы Windows, многие системы UNIX и современные системы Apple Mac могут получать доступ к серверам Microsoft с помощью этого протокола. Путь для доступа к данным подразумевает использование формата UNC (Universal Naming Convention — универсальное соглашение об именовании) вида \\сервер\имя_общего_ресурса. А при использовании внутри доменных пространств имен DFS (например, домена companyabc.com) возможно обращение вида \\companyabc.com\имя_общего_ресурса.

Первой линией защиты общих ресурсов являются права доступа к этим ресурсам. Права доступа к общим ресурсам ограничивают доступ к CD /DVD-приводам, томам FAT, томам NTFS и томам reFS. Сами права доступа к общим ресурсам ограничиваются тремя вариантами: Full Control (Полный контроль), Change (Изменение) и Read (Чтение). Права уровня Full Control позволяют пользователям управлять всеми данными и сбрасывать права доступа, права уровня Change — только управлять всеми данными, а права уровня Read — только считывать данные. Поскольку права доступа к общим ресурсам задаются не очень точно, для повышения безопасности данных лучше создавать общие папки только на томах NTFS и reFS.

В случае создания общих ресурсов на томах NTFS, к пользователю применяются как права доступа, установленные для общего ресурса, так и права доступа, установленные для папок и файлов NTFS. В Windows Server 2012 эти права доступа объединяются, и применяются наиболее жесткие из них. Например, в случае настройки общего доступа к папке `c:\users` и предоставления пользователю testuser1 права Read (Чтение) на уровне общего доступа и прав Change (Изменение) или Modify (Модификация) на уровне папки NTFS, при получении доступа к находящимся в этой общей папке данным у пользователя testuser1 будет только право Read (Чтение) . Если же этот пользователь войдёт в консоль системы и попытается получить доступ к папке `c:\UserShare` напрямую, тогда у него будут права Change (Изменение) или Modify (Модификация).

6.2.2. Пространство имен DFS

Этот метод подразумевает применение общих папок Windows в унифицированном пространстве имен. Главное отличие между стандартными общими папками Windows Server и общими ресурсами DFS состоит в том, что фактическое имя сервера маскируется унифицированным именем, в роли которого обычно выступает доменное имя Active Directory, однако в некоторых случаях имя сервера и общего ресурса могут применяться для получения доступа к данным, хранящимся на нескольких серверах. Кроме того, в случае использования DFS (Distributed File System — распределенная файловая система) лежащие в основе данные могут реплицироваться между серверами. Одним из ограничений DFS является то, что клиент, получающий доступ к

пространству имен DFS, для того чтобы иметь возможность пользоваться преимуществами DFS, а в некоторых случаях и просто получать доступ к данным, должен обязательно поддерживать DFS.

У DFS имеется много преимуществ и функциональных возможностей, которые могут упрощать доступ к данным и управление ими как для администраторов, так и для конечных пользователей. Ниже перечислены четыре основных функции DFS.

- **Унифицированное пространство имен**. Данные DFS находятся в едином имени сервера или едином имени домена.
- **Избыточность данных**. DFS может обеспечивать доступ к одному общему ресурсу, обслуживаемому на нескольких серверах, тем самым позволяя перенаправлять или переключать клиентов на другой сервер в случае невозможности установки связи с первичным сервером.
- **Автоматическая репликация данных**. DFS может настраиваться так, чтобы она использовала встроенную службу DFSR (Distributed File System Replication — репликация распределенной файловой системы) и автоматически осуществляла репликацию папок между серверами DFS для обеспечения избыточности данных или централизованного хранения данных дочерних офисов.
- **Консолидация распределенных данных**. DFS может использоваться для предоставления единого пространства имен, содержащего несколько отдельных и уникальных наборов данных, которые могут располагаться на разных серверах. Это позволяет администраторам обеспечивать доступ к существующим общим файловым ресурсам на нескольких различных файловых серверах из единого пространства имен, не прибегая к репликации и избыточным наборам данных.

Пространства имен DFS

DFS может использоваться несколькими разными способами, но обычно требует создания пространства имен DFS. В роли пространства имен DFS может выступать как имя одного сервера и общей папки, так и DNS- и NetBIOS-имя домена Active Directory и представляющей общей ресурс папки. Пространство имен DFS также известно как корень пространства имен. Пространство имен позволяет автоматически перенаправлять подключения так, чтобы пользователи об этом даже и не догадывались.

Чтобы DFS могла правильно функционировать в том, что касается перенаправления клиентов и базовых подключений, в качестве клиентов DFS должны обязательно использоваться только системы, совместимые с DFS. В сети, где поддерживаются различные версии клиентских систем Windows, Mac и UNIX, DFS должна обязательно тестироваться на всех из них и только потом внедряться в производственный процесс.

Поскольку клиенты DFS не подключаются к фактическому серверу по имени, администраторы могут перемещать общие папки на новые серверы без изменения сценариев регистрации пользователей и обозначений отображенных сетевых дисков. На самом деле данные DFS, представленные в одном

пространстве, могут размещаться на нескольких серверах для обеспечения избыточности и распределения больших объемов данных.

Автономное пространство имен DFS

Автономное пространство имен (standalone namespace) подразумевает использование имени сервера, обслуживающего пространство имен DFS. Автономные пространства имен DFS следует применять в тех случаях, когда требуется упростить доступ к файловой системе, а объем данных превышает емкость одного сервера. Автономные пространства имен DFS удобны также при замене старого файлового сервера, если все пути должны оставаться полностью функциональными.

Кроме того, создание автономных пространств имен поддерживается даже тогда, когда не существует ни одного домена Active Directory. В случае создания автономного пространства имен DFS на сервере Windows Server 2012, который является членом домена Active Directory, можно настроить DFSR.

Доменное пространство имен DFS

Доменное пространство имен DFS подразумевает использование имени домена Active Directory, членом которого является сервер этого пространства имен DFS. Доменное пространство имен DFS создается после развертывания домена Active Directory по адресу *домен*\SYSVOL для репликации групповых политик домена и папок сценариев регистрации. Доменные пространства имен DFS поддерживают репликацию с помощью как старой службы File Replication Service (Служба репликации файлов), так и новой службы DFSR.

6.2.3. Репликация DFS

Когда существует домен Active Directory, автономные и доменные пространства имен DFS поддерживают репликацию хранящихся на нескольких серверах данных DFS. Это может быть очень удобным средством для распределения приложений компании на каждом сайте или обеспечения централизованного хранения данных удаленных офисов для избыточности, выполнения резервного копирования централизованным образом и оказания поддержки пользователям, которые путешествуют и работают в разных офисах компании.

В Windows Server 2003 R2 появилась, а в Windows Server 2008 R2 была усовершенствована служба для расширения возможностей и оптимизации механизма репликации DFS. Эта служба называется Distributed File System Replication (Репликация распределенной файловой системы), или DFSR, и подразумевает использование нового протокола RDC (Remote Differential Compression — удаленное дифференциальное сжатие). Она заменяет собой унаследованную службу FRS (File Replication Service — служба репликации файлов), которая до этого применялась для репликации данных DFS. Если все указанные в группе репликации DFS серверы DFS функционируют под управлением Windows Server 2003 R2 и последующих версий, для репликации данных DFS будет использоваться служба DFSR, но если хотя бы какой-то один из них работает под управлением операционной системы более ранней версии, будет использоваться служба FRS. У этого правила существует одно исключение: системный том домена (SYSVOL) будет реплицироваться между контроллерами домена с помощью службы FRS, даже если все контроллеры функционируют под

управлением Windows Server 2012, до тех пор, пока функциональный уровень домена не будет поднят до уровня Windows Server 2012 и SYSVOL не будет перемещен из FRS в DFSR.

Механизм репликации DFS и пространства имен DFS не зависят друг от друга, но могут использоваться вместе, поскольку они обычно развертываются подобным образом. Репликация папок может настраиваться между серверами, не обслуживающими ни пространства имен DFS, ни папки пространств имен DFS, но тогда служба репликации DFS должна быть установлена на всех системах, принимающих участие в репликации. ОС Windows Server 2012 увеличивает безопасность и производительность репликации DFS, поскольку вся репликация DFS сжимается и шифруется. Обратите внимание, что поток данных не может передаваться в незашифрованном виде.

Планирование репликации DFS

Когда организация хочет, чтобы данные, хранящиеся на публикуемых в пространствах имен DFS системах Windows Server 2012, реплицировались, администраторы должны создавать пространства имен только на тех серверах, которые являются членами домена Active Directory. Репликация может настраиваться между несколькими конечными объектами, находящимися либо в папке DFS, либо на системах Windows Server 2008 или Windows Server 2012, которые не принимают участия в пространстве имен DFS. В случае определения для папки нескольких конечных объектов DFS может использовать службу FRS или DFSR для создания объектов подключений репликации и автоматической синхронизации данных между этими конечными объектами.

Первоначальный ведущий сервер

При первой настройке репликации с помощью консоли DFS и мастера создания группы репликации (New Replication Group Wizard) администратор может выбирать, какой из серверов назначения будет первоначальным ведущим сервером. Данные, находящиеся на первоначальном сервере, реплицируются в остальные конечные объекты. Для конечных объектов на серверах, не являющихся первоначальными, существующие данные пересылаются в скрытый каталог, а в текущий каталог заносятся данные, которые содержатся только в совместно используемой папке первоначального сервера. После завершения первичной репликации администратор может восстанавливать данные, пересланные в скрытую папку, обратно в рабочий каталог, что может запускать репликацию во все остальные реплики из набора реплик, если репликация является двунаправленной и ни одна из целей не настроена только для чтения. При добавлении в набор реплик дополнительных конечных объектов следует стараться начинать с пустых папок.

Промежуточная папка

Промежуточная папка (staging folder) — это место, где член репликации DFS хранит данные, которые будут реплицироваться на другие члены репликации внутри группы репликации. В полностью синхронизируемой группе репликации промежуточная папка на всех серверах будет пустой. Поскольку данные репликации будут проходить через эту папку, диск, на котором находится промежуточная папка, должен иметь достаточно свободного пространства для

вмещения промежуточной папки максимального размера и при этом иметь возможность обрабатывать дополнительную дисковую нагрузку. По умолчанию промежуточная папка находится в целевой открытой папке, в скрытом каталоге E:\Users\DfsrPrivate\Staging, если цель, к примеру, находится в E:\Users. Размер промежуточной папки для любой группы DFSR по умолчанию составляет 4 Гбайт. Узнайте, какие данные будут реплицироваться, и настройте соответствующим образом объем промежуточной папки, чтобы избежать ее переполнения.

Определение топологии репликации

В Windows Server 2012 система DFS поставляется с несколькими встроенными топологиями репликации, из которых при конфигурировании репликации между конечными объектами папок DFS и членами группы репликации администратор может выбирать наиболее подходящую. Все они вкратце описываются ниже. В общем, если организации необходима настоящая многоуровневая репликация, администратору лучше настраивать подключения и график репликации DFS в соответствии с текущими подключениями топологии репликации сайта Active Directory или уже существующей сетевой топологией.

Звезда

Смысл топологии "Звезда" (hub-and-spoke) в принципе понятен из ее названия. Один конечный объект назначается центральным (hub setver) сервером репликации, а все остальные конечные объекты автоматически становятся лучевыми (spoke server) серверами репликации и осуществляют репликацию только с этим центральным сервером. Центральный сервер имеет два подключения с каждым лучевым сервером: одно для отправки данных и одно для получения данных. Такая топология требует трех или более серверов и в случае недоступности центрального сервера подразумевает прекращение пересылки репликационных обновлений между всеми членами репликации. В Windows Server 2012 появилась возможность задавать более одного центрального объекта при создании звездообразной топологии.

Полная сетка

В случае применения топологии "Полная сетка" (full mesh) каждый конечный объект имеет соединение со всеми остальными конечными объектами в группе репликации. Это позволяет продолжать выполнение репликации между доступными членами репликации даже тогда, какой-то из членов становится недоступным. Поскольку у каждого члена имеется соединение с каждым из всех остальных членов, репликация может продолжаться даже при доступности всего лишь двух членов репликации. Использование этой топологии с наборами репликации для чтения/записи может приводить к конфликтам данных, если данные изменяются на нескольких сайтах, поэтому данную топологию следует применять с осторожностью.

6.3. Ограничения на работу с файлами

6.3.1. Обзор службы File Server Resource Manager (FSRM)

ОС Windows Server 2012 содержит средство управления файловой системой и настройки отчетности - диспетчер ресурсов файлового сервера (File Server Resource Manager — FSRM), который появился еще в Windows Server 2003 R2. Он позволяет управлять квотами на уровне томов и папок, создавать и применять политики фильтрации файлов и генерировать предупредительные уведомления и отчеты по расписанию и в реальном времени, а также классифицировать файлы и папки на базе критериев, определенных администраторами.

Средства для управления квотами на уровне томов, которые предлагались в предыдущих версиях Windows Server, сильно ограничивали администраторам способы применении квот и имели несколько недостатков. Благодаря функциональным возможностям, которые поставляются в Windows Server 2012 вместе со службой FSRM, администраторы теперь могут создавать квоты на уроне томов или папок, а также настраивать любые исключения или более жесткие ограничения на уровне подпапок. Это позволяет устанавливать стандартный размер квот, а затем применять различные политики квот к конкретным группам и пользователям.

С помощью доступной в FSRM функции фильтрации файлов, организации могут запрещать всем пользователям сохранять в хранилище сервера файлы определенных типов — например, музыку, видео или исполняемые файлы. Конечно, при необходимости эти фильтры можно переопределить с помощью исключений фильтрации.

В Windows Server 2012 FSRM имеется средство File Classification infrastructure (Инфраструктура классификации файлов). Оно позволяет запускать по расписанию задачи, которые идентифицируют и помечают или классифицируют файлы на основе местоположения их хранения и/или их внутреннего содержимого. Естественно, средство FCI может выполнять поиск только по содержимому файлов определенных типов, к которым не относятся шифрованные файлы. FCI также задействуется при развертывании динамического управления доступом (DAC) в сети.

Ниже перечислены некоторые наиболее распространенные способы применения FSRM.

- **Установка ограничений по объемам сохраняемых данных**. Администратор может устанавливать ограничение по объему пространства, которое пользователю или группе пользователей разрешается использовать для сохранения своих данных внутри системного тома или папки. Это традиционный способ ограничения объемов хранения с помощью квот, позволяющий ограничивать пользователей сохранением — например, не более 10 Гбайт файлов в сети.

- **Обеспечение гибкости ограничения хранилища для групповых данных**. Когда пользователю или группе пользователей необходимо иметь разные ограничения по объему хранения, вместо предоставления этими пользователям неограниченного доступа администратор с помощью FSRM может

расширять объемы разрешенного сверх стандартного лимита пространства внутри конкретных папок путем применения жесткой политики квот для родительской папки и либо отключения, либо применения менее жесткой политики квот для необходимой подпапки или подпапок.

• **Принудительное применение политик хранения**. FSRM позволяет администраторам не только определять политики хранения, но также принудительно применять их путем создания отчетов и генерирования уведомлений о нарушении политик и предопределенных предельных ограничений по объемам хранения в реальном времени и по расписанию, с их последующей отправкой по электронной почте, занесением в журналы событий или сохранением в специальных папках отчетов.

• **Политики фильтрации файлов**. Администраторы могут блокировать сохранение файлов определенного типа или типов. В последние годы многие организации с удивлением обнаружили, что одной из главных причин увеличения требований к объемам хранилищ данных является загрузка и сохранение конечными пользователями на файловых серверах музыки, фильмов и личных фотографий. При необходимости можно создавать исключения и применять их к отдельным подпапкам.

• **Классификации файлов**. Администраторы могут определять свойства классификации файлов и правила, которые могут позволять запускать вручную или по графику задания проверки файлов и снабжения их тегами на основе административных правил. Это может быть полезно для идентификации данных на основе характеристик использования либо по их содержимому, чтобы обеспечить повышенную безопасность и управление ответственной информацией.

6.3.2. Назначение файловых квот с помощью FSRM

Чтобы создать и настроить квоты FSRM, выполните следующие шаги.

1. Войдите в систему Windows Server 2012 с необходимым общим ресурсом и откройте диспетчер серверов.

2. В панели древовидного представления щелкните на ссылке **File and Storage Services** (Служба файлов и хранения) и в открывшемся окне щелкните на ссылке **Servers** (Серверы).

3. В панели Servers щелкните правой кнопкой мыши на нужном сервере и выберите в контекстном меню пункт **File Server Resource Manager** (Диспетчер ресурсов файлового сервера), чтобы открыть консоль FSRM.

4. В открывшемся окне консоли дважды щелкните на узле **Quota Management** (Управление квотами).

5. В панели древовидного представления выделите узел **Quotas** (Квоты).

6. В панели **Actions** (Действия) щелкните на ссылке **Create Quota** (Создание квоты).

7. В открывшемся окне **Create Quota** (Создание квоты) укажите путь для квоты, например, E:\GroupShare.

8. Выберите вариант **Auto Apply Template and Create Quotas on Existing and New Subfolders** (Автоматически применять шаблон и создавать квоты на существующих и новых подпапках).

9. В разделе окна **Quota Properties** (Свойства квоты) выберите вариант **Derive Properties from This Quota Template** (Наследовать свойства от этого шаблона квоты) и в раскрывающемся меню выберите **200 MB Limit Reports to User** (Отчеты с ограничением в 200 Мбайт для пользователя). Щелкните на кнопке **Create** (Создать), как показано на рис. 6.6.

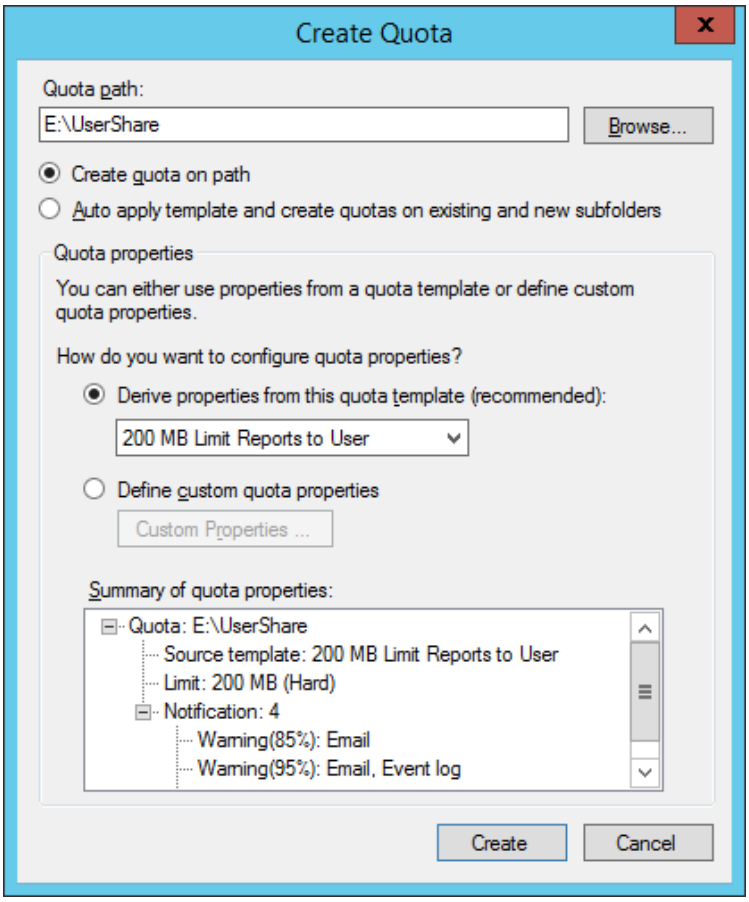

Рис. 6.6. Создание новой квоты FSRM

10. После создания квоты щелкните на ссылке **Refresh** (Обновить) в панели **Actions** (Действия).

11. После этого новая квота появится в панели задач вместе с информацией о квотах, применённых ко всем существующим подпапкам, и текущим состоянием каждой из них.

6.3.3. Скрининг файлов с помощью FSRM

Диспетчер ресурсов файлового сервера может также создавать файловые фильтры. Примененный к папке файловый фильтр инспектирует каждый подлежащий сохранению в ней файл и либо разрешает, либо запрещает пользователю сохранять этот файл на основе указанных в нем параметров. Файловый фильтр блокирует возможность записи файлов как внутри папки, так и во всех ее подпапках. Например, организация может разрешить сохранение всех неопределенных документов и запретить сохранение аудио- и видеофайлов

с расширениями *.mp3 и *.mpg просто путем применения файлового фильтра, содержащего два этих типа файлов для определенной папки и набора папок.

Создать файловый фильтр можно с помощью перечисленных ниже шагов.

1. Откройте диспетчер FSRM и разверните узлы в нем.

2. Дважды щелкните на элементе File Screening Management (Управление фильтрацией файлов).

3. Выделите узел File Screens (Файловые фильтры). В панели Actions (Действия) щелкните на ссылке Create File Screen (Создать файловый фильтр).

4. В окне Create File Screen (Создание файлового фильтра) укажите путь для файлового фильтра, например, e:\UserShare.

5. В разделе File Screen Properties (Свойства файлового фильтра) окна выберите вариант Derive Properties from This File Screen Template (Наследовать свойства от этого шаблона файлового фильтра), если хотите применить шаблон, или вариант Define Custom File Screen Properties (Определить специальные свойства для файлового фильтра), если хотите создать специальный фильтр. Для данного примера выберите вариант Derive Properties from This File Screen Template и в раскрывающемся списке выберите пункт Block Audio and Video Files (Блокировать аудио- и видеофайлы), как показано на рис. 6.7. Затем щелкните на кнопке Create (Создать), чтобы создать новый файловый фильтр.

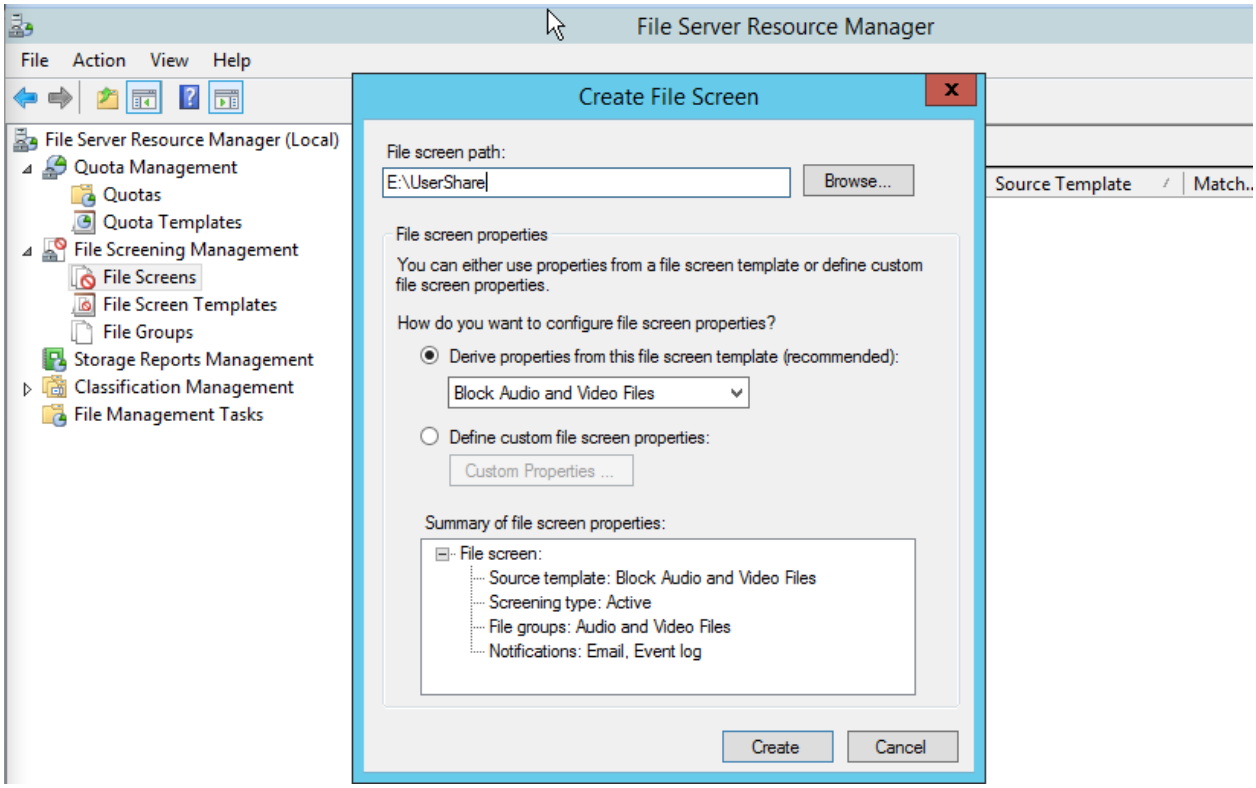

Рис. 6.7. Создание нового файлового фильтра

6.4. Организация работы с документами с помощью SharePoint Server

6.4.1. Основные функции SharePoint Server

Microsoft SharePoint — это коллекция программных продуктов и компонентов, включающая в себя:

- набор веб-приложений для организации совместной работы;
- функциональность для создания веб-порталов;
- модуль поиска информации в документах и информационных системах;
- функциональность управления рабочими процессами и систему управления содержимым масштаба предприятия;
- модуль создания форм для ввода информации;
- функциональность для бизнес-анализа.

SharePoint позволяет гибко настроить права доступа к сайтам и файлам для обеспечения безопасности. Создаваемые на платформе «SharePoint» сайты могут быть использованы в качестве хранилища информации, знаний и документов, а также использоваться для исполнения облегчающих взаимодействие веб-приложений, таких как форумы, вики и блоги. Также в SharePoint можно создавать календари и задачи (с диаграммами Ганта), что дополняет календарь и задачи в Outlook.

Вообще, SharePoint — это платформа для разработки, а значит, ее можно дополнять, настраивать, интегрировать. То есть, все вышесказанное касается базовой функциональности SharePoint.

Социальная сеть

У каждого пользователя SharePoint есть профиль — личная страница с фотографией, персональными данными. На этой странице можно найти связи человека с другими сотрудниками — например, кто работает с ним в отделе. При этом поиск SharePoint позволяет находить не только документы, но и персональные страницы людей. Это полезно, когда не знаешь, у кого в компании можно найти ответ на свой вопрос.

Бизнес-процессы и формы

В SharePoint можно настраивать целые бизнес-процессы, которые инициируются при заполнении формы. Например, кто-то ввел в форму заявку на кредит — автоматически формируется документ-заявка с данными из формы, поступает ответственному сотруднику на проверку, после проверки — на утверждение руководителю, после утверждения — автоматически отправляется уведомление человеку, который заполнял форму.

Управление записями

Записи — это, например, сообщения в мессенджере на форуме или электронные заметки — в общем, неструктурированная информация, которая обычно не фигурирует в системах управления, но может быть весьма полезна для компании. SharePoint умеет искать такие записи и индексировать, чтобы можно было их легко найти.

Отчеты

SharePoint умеет брать данные из Excel-файлов, баз данных, онлайн источников и создавать различные аналитические отчеты.

Доступ к бизнес-приложениям

SharePoint позволяет создавать портлеты (которые в SharePoint называются Web Parts) для интеграции с корпоративными приложениями. При этом для сотрудника создается веб-интерфейс, с помощью которого он может получить доступ, например, к своему почтовому ящику или CRM-системе прямо из SharePoint. Это очень удобно, т.к. не нужно открывать множество приложений, регистрироваться в каждом и переносить информацию из одного в другое. SharePoint делает это автоматически.

6.4.2. Логическая организация фермы SharePoint

В следующем списке будут перечислены стандартные функциональные возможности, включенные в SharePoint. Этот список не полон, однако он дает общее представление.

• **Библиотеки документов**. Этот базовый компонент сайта SharePoint предназначен для хранения документов и управления ими, и позволяет администратору добавлять в библиотеку дополнительные столбцы данных (они называются метаданными), а также создавать специальные представления, отслеживать версии документов и управлять доступом на уровне документа. Библиотека документов предлагает множество других функциональных возможностей, например, требование завершить работу над документом, прежде чем его можно будет редактировать, или генерация извещений с отправкой сообщения по электронной почте, если будут соблюдены некоторые условия, такие как изменение документа. Другие стандартные библиотеки включают библиотеку форм, библиотеку слайдов и библиотеку вики-страниц.

> ***Метаданные*** *— это данные о данных. Поэтому, например, документ Microsoft Word имеет метаданные, связанные с ним (фамилия автора, дата создания и дата изменения документа). Библиотеки документов SharePoint Foundation позволяют определять другие столбцы, которые могут содержать самую разнообразную информацию, имеющую отношение к документу.*

• **Списки**. Этот компонент сайта SharePoint может принимать многие формы, однако по своей сути он представляет собой набор данных, представленных в виде электронной таблицы, которые могут использоваться для решения практически любых задач. Например, стандартные списки включают объявления, календари, списки адресатов, доски обсуждений, задачи и опросы.

• **Веб-страницы и веб-части**. Веб-страницы SharePoint — это основные строительные блоки среды SharePoint, т.к. они представляют данные, инструменты и веб-части пользователям среды, которая отображается в браузере. Веб-части — это модульные компоненты, которые можно помещать на страницы для выполнения функций вроде вывода данных из библиотек документов или списков, с сайта погоды или биржевых сводок. Пользователи могут создавать и настраивать новые страницы вроде вики-страниц, предоставлять контент, ориентированный на конкретных пользователей

(который часто называется досками обсуждения, dashboard), и выставлять текст и графику для обсуждений.

• **Сайты и рабочие пространства**. Сайты и рабочие пространства по своей сути являются группами списков, библиотек и базовых страниц веб-частей, которые предлагают пользователям широкие функциональные возможности. Например, можно создать сайт для учета кадров предприятия или для отдела информационных технологий; можно создать рабочее пространство, которое позволит пользователям совместно работать над документом; рабочее пространство можно создать и для определенного события, например, для квартального собрания компании.

• **Инструменты управления сайтом**. Они представлены в различных формах, включая инструменты для редактирования страниц с использованием браузера, инструменты для управления подсайтами, а также инструменты управления сайтами верхнего уровня. Имеются простые средства для индивидуализации сайта (изменение цветов и шрифтов), и можно включать и отключать компоненты сайта, чтобы разрешать или запрещать пользователям доступ к различным инструментам. Организации часто разрешают "подготовленным пользователям" доступ к таким инструментам, чтобы распределить администрирование сайтов и снизить нагрузку на IT-персонал.

• **Инструменты центра администрирования (Central Administration)**. Эти инструменты позволяют администратору SharePoint конфигурировать сервер или серверы с целью обеспечения должной их работы, или для выполнения резервирования и восстановления данных. Здесь можно управлять приложениями-службами SharePoint, а также настраивать параметры поиска, связи с Active Directory и вносить изменения, связанные с производительностью и конфигурированием, на многих уровнях структуры SharePoint. В Microsoft также рекомендуют использовать средства SharePoint для решения более сложных или повторяющихся задач. IT-персонал обычно сохраняет контроль над такими средствами, поскольку они могут повлиять на общую надежность и эффективность всей среды SharePoint.

• **Служба связи с бизнес-данными**. В составе SharePoint предлагается служба связи с бизнес-данными (Business Data Connectivity Service — BDCS), которая позволяет подключаться к внешним источникам данных, таким как веб-служба, база данных SQL Server или другая реляционная база данных, сохраняя защиту этих источников. Ряд специальных веб-частей позволяет выводить эти данные в виде сложных инструментальных панелей.

Логическая архитектура SharePoint 2016 состоит из следующих компонентов:

• **Ферма**. Ферма SharePoint работает на одном или нескольких серверах и обычно состоит из нескольких веб-приложений и сервисных приложений. База данных конфигурации фермы хранит данные веб-приложения и ассоциации сервисных приложений внутри фермы, и на ферму имеется только одна база данных конфигурации фермы.

• **Сервисные приложения**. Сервисные приложения предоставляют специфические функции веб-приложениям в ферме, такие как служба профилей пользователей, поиск, службы Excel или служба управляемых метаданных. Администраторы создают и настраивают сервисные приложения на уровне

фермы, но можно связать одно или несколько сервисных приложений только с конкретными веб-приложениями, чтобы контролировать, какие веб-приложения могут использовать определенные функции или функции. Сервисные приложения подключаются к веб-приложениям через прокси-сервер серверного приложения или прокси-группу приложения. Каждое служебное приложение представляет собой некоторый управляемый код в SharePoint, который запускается пулом приложений в Microsoft Internet Information Services (IIS).

• **Веб-приложения**. Веб-приложение в SharePoint может содержать одну или несколько коллекций сайтов в одной или нескольких базах данных, которые выполняются под общим именем сервера или заголовком хоста IIS, например, http://sharepoint.contoso.com. Веб-приложение может иметь более одного заголовка хоста, который может поддерживаться более чем одним альтернативным сопоставлением доступа. Все семейства сайтов в веб-приложении могут использовать только альтернативное сопоставление доступа, настроенное в родительском веб-приложении. Веб-приложения также предоставляют ссылку на соответствующий объект веб-сайта в IIS и ссылку на конкретные базы данных контента в SQL Server для хранения коллекций сайтов и связанного с ними контента. Для каждого веб-приложения также требуется папка в структуре файлов IIS каждого веб-интерфейса для хранения связанных кодов, решений, шаблонов и файлов веб-конфигурации.

• **База данных контента**. Каждая база данных контента работает на SQL Server и сохраняет контент из одного или нескольких семейств сайтов. База данных контента может быть связана только с одним веб-приложением одновременно.

• **Коллекция сайтов**. Коллекция сайтов состоит из одного или нескольких сайтов SharePoint, которые организованы как иерархия в семействе сайтов. Когда вы создаете новый семейство сайтов, в семействе сайтов создается специальный сайт, известный как сайт верхнего уровня. Сайт верхнего уровня является самым высоким сайтом в иерархии этого конкретного семейства сайтов и имеет самый короткий URL всех сайтов в пределах этого семейства сайтов. Кроме того, некоторые настройки семейства сайтов доступны только на странице настроек сайта верхнего уровня.

Хотя все коллекции сайтов в одном и том же веб-приложении обычно используют одно и то же альтернативное сопоставление доступа, иерархия между коллекциями сайтов отсутствует: один набор сайтов не наследует безопасность, навигацию или другие настройки из другой коллекции сайтов (хотя у двух коллекций сайтов могут быть некоторые аналогичные настройки при управлении сервисным приложением). Это означает, что каждый набор сайтов ведет себя как граница безопасности. Например, хотя коллекция сайтов на http://sharepoint.contoso.com/sites/hr оказывается ниже коллекции сайтов по адресу http://sharepoint.contoso.com/ (из-за аналогичного, но более длинного URL), первый набор сайтов не наследует никаких настроек из второго семейства сайтов.

• **Сайт**. Сайты SharePoint создаются как часть иерархической структуры семейства сайтов, начиная с сайта верхнего уровня. Когда вы создаете новый сайт, структура сайта и макет будут основываться на предопределенном шаблоне

сайта, который обычно основывается на типе использования сайта, например, для совместной работы, хранения документов или BI. Сайты SharePoint, аналогичные папкам в общих папках сетевых файлов в общем сетевом файле, часто используются для организации контента, имеющего сходную цель или использование, например, для отдела или проекта. Аналогичным образом, организации могут использовать сайты для организации контента, такие как создание сайта для отдела или сайта для проекта.

Сайты могут содержать больше, чем просто файлы, потому что вы можете иметь списки, рабочие процессы, содержимое веб-страницы или другие типы информации, чтобы обеспечить лучший опыт для пользователей. Сайты могут наследовать параметры, такие как разрешения и поведение навигации с родительского сайта. Как правило, сайты содержат один или несколько списков или библиотек, которые сайт использует для организации и хранения содержимого сайта.

Обзор информационной архитектуры SharePoint 2016

Когда вы планируете развертывание SharePoint 2016, вам следует потратить некоторое время на планирование классификации и классификации информации, хранящейся в списках и библиотеках SharePoint. Эта классификация и классификация составляют большую часть вашей информационной архитектуры и являются важной частью помощи пользователям в поиске информации, необходимой для более эффективной работы.

Метаданными в SharePoint называется информация, используемая для категоризации и классификации контента. Метаданные в SharePoint могут содержать различные категории или классификации, такие как отделы, местоположения, проекты или любые другие подходящие критерии.

Для поддержки использования метаданных в рамках информационной архитектуры организации SharePoint использует следующие функции:

• **Столбцы сайта**. Вы можете создавать столбцы сайта на уровне сайта для хранения метаданных в качестве дополнительного столбца, который может быть применен к списку или библиотеке внутри или ниже этого сайта в иерархии. Столбцы сайта могут использовать различные типы, такие как текст, выбор, число, дата и время, личность, группа или вычисляемые значения. Создание столбца сайта на сайте верхнего уровня делает этот столбец доступным для всех списков и библиотек в коллекции сайтов. Однако столбцы сайтов нельзя унаследовать от одного коллекции сайтов к другой.

• **Наборы терминов**. Служба управляемых метаданных в SharePoint позволяет создавать наборы терминов для использования в качестве метаданных в списках и библиотеках. Наборы терминов представляют категории или классификации метаданных с определенным количеством терминов, которые могут применяться в качестве метаданных для элементов в списках или библиотеках SharePoint.

Поскольку управляемые метаданные являются сервисным приложением в SharePoint, вы можете создавать глобальные наборы терминов, которые пользователи могут применять в любом семействе сайтов фермы. Чтобы пользователи могли применять термины из набора терминов, вам необходимо

создать столбец списка, библиотеки или сайта, в котором указан управляемый термин метаданных, заданный в качестве источника. Кроме того, в SharePoint 2016 вы можете использовать наборы управляемых метаданных для навигации по сайту.

• **Типы контента**. Вы используете типы контента для определения типа элемента или документа, например, бизнес-плана или бюджета. Типы контента ведут себя как особый тип шаблона, который может содержать параметры шаблона файла, сайта, рабочего процесса и политики управления информацией. Это означает, что везде, где вы используете этот тип контента, будет стандартное требование для контента и метаданных. Как и столбцы сайта, типы контента управляются на уровне семейства сайтов.

• **Наборы документов**. Наборы документов являются типом контента и предназначены для сопоставления связанных документов, как с точки зрения организации, так и часто в рамках бизнес-процесса. Наборы документов представляют собой интерфейс специализированных папок для пользователей, тем самым предоставляя пользователям привычную структуру для организации информации. Этот интерфейс папок предоставляет расширенные возможности, такие как возможность применения изменений метаданных к документам в наборе.

• **Основанные на местоположении метаданные по умолчанию**. Чтобы пользователи могли работать с метаданными, сохраняя привычную структуру для организации документов, вы можете включить определенные папки в библиотеке документов, чтобы применять значения по умолчанию к определенным полям или столбцам метаданных.

6.4.3. Иерархия объектов

Типичная среда SharePoint состоит из нескольких компонентов и имеет четкую структуру. На рис. 6.8 показана базовая логическая структура среды SharePoint.

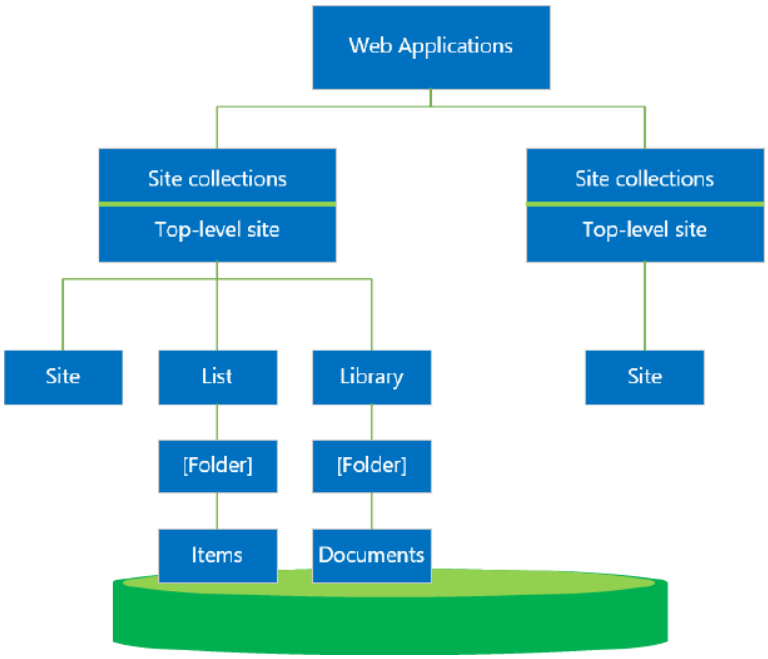

Рис. 6.8. Логическая структура SharePoint

Рассмотрим компоненты типичной среды SharePoint:

• **Веб-приложение** — это компонент самого высокого уровня логической структуры внутри фермы. Ферма может иметь одно или несколько веб-приложений.

• В веб-приложении есть одна или несколько **коллекций сайтов**. У коллекций сайтов есть единый URL.

• В коллекции сайтов содержится один или несколько **сайтов**. Когда вы создаете коллекцию сайтов, вы также создаете сайт верхнего уровня в этой коллекции сайтов. Ниже того, что сайт верхнего уровня может быть одним или несколькими дополнительными сайтами, обычно называемыми subsites.

• Сайт обычно содержит **списки** и **библиотеки**.

• Списки и библиотеки содержат **элементы** и **документы**, которые могут содержаться в **папках**.

• Коллекция сайтов и весь контент размещаются в **базе данных контента**. Может быть одна или несколько баз данных контента, связанных с веб-приложением.

Веб-приложения SharePoint 2016

Веб-приложение в SharePoint 2016 является веб-сайтом Microsoft Internet Information Services (IIS), который действует как логическая единица для всех создаваемых коллекций сайтов. Поэтому перед созданием любых коллекций сайтов вам необходимо создать веб-приложение. При создании веб-приложения он представлен веб-сайтом IIS и данными конфигурации SharePoint и связан с его собственным или общим пулом приложений (application pool).

Характеристики веб-приложения

Веб-приложения имеют следующие характеристики:

• Вы используете веб-приложения для изоляции содержимого, процессов, функций и пользователей.

• Вы можете разделить контент, доступный анонимным пользователям из контента, доступ к которому осуществляется аутентифицированными пользователями, или контента, доступного для партнеров из контента, доступного для сотрудников, путем размещения контента в отдельных веб-приложениях.

• Каждому веб-приложению может быть присвоено уникальное доменное имя, которое помогает предотвратить атаки на межсайтовый скриптинг.

• Вы можете назначить уникальный пул приложений для веб-приложения, которое изолирует его процессы.

• При создании нового веб-приложения вы также создаете новую базу данных контента, которая определяет метод проверки подлинности, используемый пулом приложений для подключения к базе данных.

• Когда вы создаете новое веб-приложение, вы указываете метод проверки подлинности, используемый для подключения к веб-сайту IIS.

• SharePoint 2016 предоставляет набор сервисных приложений, доступных для каждого веб-приложения. Вы можете выбрать, какие сервисные приложения вы хотите использовать для каждого создаваемого веб-приложения, связав веб-

приложение с прокси-группой или указав собственный набор приложений-приложений для веб-приложения.

- Политики могут быть однозначно определены для каждого веб-приложения.

Веб-приложения и базы данных контента

Коллекция сайтов и весь ее контент, включая документы и файлы в библиотеках документов, элементах списка и свойствах веб-частей, размещаются во внутренней базе данных контента. Может быть одна или несколько баз данных контента, связанных с веб-приложением. Содержимое всех сайтов коллекции сайтов хранится в базе данных контента. Коллекция сайтов не может содержать более одной базы данных контента, но при необходимости вы можете перемещать базу данных контента, чтобы улучшить производительность SQL Server или из-за проблем с ограничением размера. Единственный способ хранить сайты в отдельных базах данных контента — это размещать сайты в отдельных семействах сайтов.

Веб-приложения и сервисные приложения

Веб-приложение связано с приложением службы через соединение с сервисным приложением, также называемое прокси-сервером приложения. Соединения приложений-служб добавляются в группу подключений приложений-служб, также известную как прокси-группа приложения. При создании веб-приложения один из шагов настройки, которые вы выполняете, заключается в выборе группы соединений приложения-службы или прокси-группы для подключения к веб-приложению. Веб-приложение может быть подключено к прокси-группе по умолчанию, что и происходит по умолчанию, или вы можете выбрать настраиваемую прокси-группу; однако вы можете создать только одну настраиваемую прокси-группу для каждого веб-приложения в ферме.

Типы зон веб-приложений

Часто у вас есть веб-сайт IIS, который вы хотите предоставить для нескольких типов пользователей, таких как пользователи интрасети и пользователи Интернета. Поскольку для каждого типа пользователя вам обычно требуются разные механизмы аутентификации, вы можете расширить свое веб-приложение, чтобы сделать его доступным из разных URL-адресов. Один из способов добиться этого — расширить веб-приложение в разные зоны.

В SharePoint 2016 существует пять возможных зон для веб-приложения:

- Default
- Intranet
- Internet
- Custom
- Extranet

> *Примечание. Эти имена зон произвольны и не имеют никакого особого значения. Нет никаких свойств или условий, связанных с именами зон.*

Зона по умолчанию (Default) создается при первом создании веб-приложения; другие зоны создаются при расширении веб-приложения в одну из этих зон.

> *Примечание. Можно только выбрать каждый тип зоны один раз в веб-приложении. Например, после того, как вы расширили веб-приложение в*

зону Интернета, вы не можете расширить веб-приложение в другую зону Интернета.

Когда вы расширяете веб-приложение в одну из этих зон, вы фактически создаете новый отдельный веб-сайт IIS, который обслуживает тот же контент, что и другие веб-сайты в вашем веб-приложении, но каждый из них имеет свой собственный уникальный URL-адрес для подключения и может также использовать разные методы аутентификации.

Коллекции сайтов в SharePoint 2016

Коллекция сайтов — это группа веб-сайтов SharePoint, на которых есть общие владельцы и администраторы верхнего уровня, а также общие настройки, такие как квоты и блокировки. При создании семейства сайтов вы также создаете сайт верхнего уровня в семействе сайтов.

Вы можете создать любое количество подсайтов в иерархии под сайтом верхнего уровня, а дочерний узел может наследовать разрешения и навигацию со своего родительского сайта или вы можете указать их непосредственно на уровне дочерних сайтов. Коллекции сайтов должны создаваться администраторами семейства сайтов, но подсайты могут быть созданы всеми пользователями, которым было делегировано право на это.

Шаблоны сайтов

Когда вы создаете новый сайт в SharePoint 2016, вы можете начать с чистого сайта верхнего уровня, выбрав Custom (Пользовательский) в качестве шаблона, а затем выбрать шаблон позже. Однако чаще всего выбирается шаблон, такой как сайт команды (Team Site) или издательский портал (Publishing Portal), на котором основывается новый сайт. Шаблоны состоят из компонентов сайта, таких как страницы, списки и библиотеки, которые поддерживают потребности организации, такие как совместная работа, публикация контента, управление записями и бизнес-аналитика.

Шаблоны сайтов, доступные в SharePoint 2016, сгруппированы по следующим категориям:

- Collaboration. Эта категория содержит следующие шаблоны:
  - Team Site
  - Blog
  - Developer Site
  - Project Site
  - Community Site
- Enterprise. Эта категория содержит следующие шаблоны:
  - Document Center
  - eDiscovery Center
  - Records Center
  - Business Intelligence Center
  - Enterprise Search Center
  - My Site Host
  - Community Portal

- Basic Search Center
- Visio Process Repository

- Publishing. Эта категория содержит следующие шаблоны:
  - Publishing Portal
  - Enterprise Wiki
  - Product Catalog
- Custom. Select this category to create a blank site and select a template later.

Обзор архитектуры сервисных приложений

Сервисные приложения предоставляют пользователям функциональные возможности в SharePoint 2016. Это включает в себя доступ к функциональности приложений с Microsoft Access, графикой Microsoft Visio или базовыми службами, такими как служба управляемых метаданных или службы Microsoft Business Connectivity Services (BCS). Структура архитектуры сервисного приложения в SharePoint 2016 такова, что архитекторы могут выбирать только те сервисы, которые необходимы для доставки бизнес-решения.

С точки зрения основного управления сервисное приложение имеет следующие компоненты:

- административный интерфейс, с помощью которого вы можете управлять связанным сервисным приложением;
- пул приложений;
- база данных служб или базы данных, в зависимости от требований службы;
- один или несколько физических экземпляров службы, выполняющихся на физическом сервере.

Структура предоставления сервиса немного сложнее. Служебное приложение — это термин для объектов, предлагаемых в SharePoint 2016, для обеспечения функциональности для пользователей. Оно состоит из следующих элементов:

- **Экземпляр службы**. Экземпляр службы — это двоичные файлы, которые реализуют требуемую функциональность. Вы можете увидеть экземпляры службы, запущенные на сервере, на странице «Службы на сервере» в Центре администрирования. Список служб, показанных на этой странице, включает в себя базовые службы, такие как служба PerformancePoint и службы доступа, которые относятся к приложению службы доступа к службам SharePoint и службе PerformancePoint Service Application. Они обеспечивают функциональность для пользователей сервисных приложений. На странице «Службы на сервере» есть также такие службы, как коннектор Lotus Notes и Центральное администрирование.

- **Экземпляр сервера службы**. Это сервер (или серверы) на ферме, на котором выполняется служба. Не все службы имеют несколько экземпляров сервера. Некоторые службы могут работать только на одной сервере на ферме. Для служб, которые могут иметь несколько экземпляров серверов, обеспечивается балансировка нагрузки round-robin.

• **Конечная точка сервисного приложения**. Это файл Windows Communication Foundation (WCF) или ASP.NET Web Services Source (ASMX), который опубликован для связи с приложением службы.

• **Сервисное приложение**. Вы можете настроить эту услугу на странице «Управление сервисными приложениями». Вы можете создать несколько экземпляров сервисного приложения. Вы можете настроить большинство из них либо через пользовательский интерфейс (UI) сайта центра администрирования, либо через Windows PowerShell. Некоторые могут быть настроены только с помощью Windows PowerShell. Сервисные приложения являются глобальными для фермы.

• **Сервисное подключение или прокси сервисного приложения**. Это обеспечивает соединение между сервисом и веб-приложением, которое потребляет услугу.

Пользователь службы использует эти услуги. Этот термин включает веб-приложения, веб-части и другие клиенты, которые могут потреблять услуги.

Чтобы сервисное приложение обращалось к конкретному веб-приложению, оно должно использовать соединение с сервисным приложением (прокси). Прокси-сервер может создаваться автоматически при создании нового сервисного приложения. Вы можете группировать несколько прокси вместе, которые затем называются группой соединений сервисного приложения (прокси-группы). При создании веб-приложения вы указываете прокси-группу сервисного приложения (группа по умолчанию называется Default). Большинство сервисных приложений имеют одну или несколько связанных баз данных. Системные имена для этих баз данных нелегко сопоставить с сервисными приложениями. Для упрощения управления и распознавания вы должны определить свои собственные имена баз данных для своих баз данных сервисных приложений при их создании. Вы должны знать о потенциальном размере, до которого эти базы данных могут вырасти.

Обычно настраиваемые приложения для корпоративных сервисов

Есть несколько сервисных приложений, которые почти каждый администратор SharePoint 2016 настроит как минимум один раз. Это связано с тем, что они предлагают функциональные возможности, которые популярны у бизнес-пользователей, или они являются сервисными приложениями, от которых зависят другие популярные сервисные приложения. Сервисные приложения, которые популярны среди бизнес-пользователей, включают:

• **Службы Access**. Это служебное приложение добавляет базу данных Access 2013 или более поздней версии в Microsoft SQL Server как свою собственную базу данных в комплекте с представлениями и обрабатывает ее в SharePoint для доступа пользователей к ней. Хотя он не может легко поддерживать оповещения или рабочие процессы, он использует возможности SQL (или Microsoft Azure для SharePoint Online) для более быстрой и надежной работы.

• **Службы Access 2010**. Это служебное приложение публикует базу данных Access 2010 в виде веб-базы данных для SharePoint 2016, преобразуя таблицы базы данных в списки. Хотя обе службы доступа используют модель приложения SharePoint, уведомления и рабочие процессы более совместимы с этим типом

приложения. Вы не можете создать веб-базу данных Access 2010 с помощью Access 2013 или более поздней версии, но вы можете просматривать и редактировать ее. Эта услуга предоставляется в первую очередь для обратной совместимости.

• **Служба поиска**. Это служебное приложение обеспечивает функции поиска в корпоративной среде в вашей среде. SharePoint Server 2013 реинжиниринга Поиск включает функциональность FAST. Поиск SharePoint 2016 специально поддерживает гибридную модель, позволяя (при условии, что он имеет правильную конфигурацию) пользователям одновременно искать контент как в локальной среде, так и в облаке.

• **Службы PerformancePoint**. Это служебное приложение предоставляет инструменты для разработки параметров пользовательского интерфейса Business Intelligence, таких как информационные панели, оценочные карточки и ключевые показатели эффективности, чтобы отслеживать и анализировать эффективность бизнеса.

• **Службы Visio Graphics**. Эта услуга предоставляет пользователям возможность отображать диаграмму Visio в веб-браузере. Содержимое также может быть обновлено и пересчитано для диаграмм, размещенных на сайте SharePoint.

Услуги, предлагающие поддерживающие функции, от которых часто зависят другие приложения-службы, включают:

• **Служба настроек подписки**. Эта услуга предлагает предоставление коллекций сайтов арендаторов. Локальная ферма требует, чтобы эта служба работала в гибридном сценарии с SharePoint Online. Это позволяет управлять отдельными коллекциями сайтов администратором-арендатором (или группой администраторов). Ресурсы могут быть изолированы между арендаторами, такими как поиск или управляемые метаданные, путем запуска этих сервисных приложений в режиме секционирования. Не все сервисные приложения поддерживают секционирование.

• **Службы бизнес-связи (Business Connectivity Services)**. BCS обеспечивает доступ к данным внешних систем, чтобы приложения SharePoint 2016 могли его использовать. Несколько сервисных приложений тесно связаны с BCS, такими как служба профилей пользователей, которая обеспечивает доступ к информации пользователя, хранящейся на внешних системах.

• **Служба управляемых метаданных**. Служба управляемых метаданных предоставляет возможность использования функций метаданных, таких как управляемые метаданные, наборы терминов и типы контента в веб-приложениях и коллекциях сайтов.

• **Служба безопасного хранения (Secure Store Service)**. Эта служба предоставляет базу данных, в которой хранятся учетные данные аутентификации. Другие сервисные приложения используют эту услугу для обеспечения внешнего доступа к данным, включая службы BCS и службы PerformancePoint.

• **Служба состояния (State Service)**. Эта служба предоставляет временное хранилище данных пользовательских сеансов для приложений SharePoint Server.

Она необходима для других сервисных приложений, включая Visio Graphics Services и PerformancePoint Services. Вы можете настроить службу состояния только через Windows PowerShell или с помощью мастера настройки через Центральное администрирование.

• **Служба профилей пользователей**. Эта служба предоставляет возможность создавать и администрировать профили пользователей, доступные из нескольких сайтов и ферм. Пользовательские сайты и другие локальные социальные функции зависят от этого приложения-службы. Во время выпуска SharePoint 2016 использует Forefront Identity Manager для работы, но это будет пересмотрено в течение жизненного цикла продукта, и оно будет заменено автономным менеджером идентификации под названием Microsoft Identity Manager (MIM).

• **Служба управления приложениями**. Это служебное приложение предоставляет администраторам возможность управлять надстройками SharePoint, доступными с SharePoint 2016. Организации могут приобретать приложения у внешнего поставщика или разрабатывать их внутренне. Служба управления приложениями проверяет права доступа пользователей и лицензию на использование приложений.

• **Служба машинного перевода**. Это служебное приложение подключается к службе перевода Bing для обеспечения автоматического перевода языковой версии веб-страницы, так что контент с одного сайта может быть автоматически переведен на другой язык.

Рабочий процесс сервисного приложения

Как правило, сервисные приложения предоставляют пользователям функции обслуживания. Когда пользователь делает запрос на обслуживание из браузера, запрос, например, поиск по ключевым словам, отправляется через сервер Web Front End (WFE).

Сервер WFE отправляет запрос серверу приложений, который обслуживает сервисное приложение. Архитектура сервисного приложения в SharePoint 2016 позволяет нескольким серверам использовать экземпляры одного и того же сервисного приложения, поэтому часто применяют программный балансировщик нагрузки, который направляет запросы на один из серверов.

Все коммуникации используют WCF, поэтому прямой доступ к базам приложений приложений отсутствует. По умолчанию связь между веб-серверами и сервисными приложениями в ферме происходит с использованием HTTP, но вы можете выбрать либо HTTP (порт 32843), либо HTTPS (порт 32844). Сторонние компании, которые разрабатывают сервисные приложения, могут также реализовать NetTcpBinding (порт 32845) для обеспечения высокопроизводительной связи с клиентами WCF. Как правило, NetTcpBinding — лучший вариант для служб, работающих внутри брандмауэра, например, на сайте интрасети. Администраторы могут использовать страницу «Службы приложений» для изменения протокола и привязки портов для каждого приложения-службы.

Связь между сервисными приложениями и SQL Server осуществляется через стандартные порты SQL Server или порты, которые вы настраиваете для связи SQL Server.

Подключение прикладного приложения (прокси)

При развертывании сервисного приложения вы создаете соединение с сервисным приложением. Это соединение более широко известно как прокси. Прокси-сервер управляет информацией о соединении, чтобы сервисное приложение могло связываться с запросами на обслуживание от пользователей услуг, таких как веб-части. Вы можете связывать сервисные приложения с отдельными веб-приложениями.

Это означает, что у вас есть гибкость для развертывания нескольких экземпляров сервисного приложения, которые вы можете выделить для соответствия требованиям производительности или безопасности. Вы должны помнить, что по умолчанию сервисные приложения связаны со всеми веб-приложениями на ферме, поэтому вам необходимо явно сопоставить сервисные приложения веб-приложениям. Вы можете управлять прокси через центральное администрирование или с помощью Windows PowerShell.

Прокси-группы сервисных приложений

SharePoint 2016 группирует сервисные приложения для потребления веб-приложениями через прокси-группы. Это просто наборы служебных приложений, которые можно развернуть в разных веб-приложениях. Это может показаться тривиальным, но это важный механизм проектирования для архитекторов решений для группировки и изоляции сервисных приложений.

По умолчанию большинство сервисных приложений помещаются в группу по умолчанию. Это означает, что все пользователи в веб-приложениях, которые потребляют службы из группы по умолчанию, имеют доступ к членам прокси-группы.

Однако вы можете создавать настраиваемые группы, к которым вы можете добавлять сервисы, которые вы хотите предоставить определенному веб-приложению. Когда вы создаете веб-приложение и выбираете настраиваемую группу, только это веб-приложение может использовать эти службы, поскольку эта настраиваемая группа уникальна для этого веб-приложения. Вы также можете создавать новые прокси-группы. Разница между созданием новой прокси-группы и использованием настраиваемой прокси-группы заключается в том, что вы можете применить новую прокси-группу к нескольким веб-приложениям.

Пулы приложений

Для сервисных приложений требуется, чтобы пул приложений функционировал. Для доступа к ресурсам, особенно базам данных, для пулов приложений требуется учетная запись службы (обычно управляемая учетная запись в SharePoint). Вы можете развернуть сервисные приложения в разных пулах приложений для обеспечения изоляции процесса. Однако, если вы хотите оптимизировать производительность своей фермы, вы должны развернуть сервисные приложения только для одного пула приложений.

Как уже упоминалось, вы можете использовать другой пул приложений для сервисных приложений для достижения физической изоляции. Другими словами, чтобы убедиться, что сервисное приложение будет как можно больше изолировано от других сервисных приложений, вы можете настроить экземпляр

для запуска на своем собственном сервере SharePoint 2016, используя собственную учетную запись службы и процессы для работы. Изолирование сервисного приложения собственным пулом приложений гарантирует, что он будет работать, если какой-либо из остальных пулов приложений прекратится. Это позволяет вам легко устранить проблему сервисного приложения, отслеживая действия этого пула приложений. Однако, чтобы сохранить ресурсы сервера, вы должны делать это, только если для этого есть необходимость.

Пулы приложений и прокси-группы имеют мало общего друг с другом, за исключением того факта, что вы используете их для группировки сервисных приложений. Сервисные приложения, которые не требуют изоляции процессов друг от друга, могут совместно использовать пулы приложений для сохранения ресурсов сервера. Вы используете прокси-группы для объединения сервисных приложений для управления сервисными приложениями, связанными с их соответствующим веб-приложением.

6.4.4. Типы содержимого, теги и ключевые слова.

Вы можете маркировать или классифицировать информацию, чтобы организовать ее и облегчить поиск и работу. Вы можете применять метаданные, которые могут быть категорией, классификацией или тегом, для файлов и элементов в Microsoft SharePoint 2016 для организации вашего контента и упрощения работы с ним.

В большинстве организаций наиболее эффективным способом реализации метаданных является определенная таксономия, которую вы стандартизировали с помощью различных заинтересованных сторон. Это позволяет пользователям выбирать условия метаданных из предопределенного списка, что обеспечивает стандартные результаты по всей организации.

SharePoint 2016 может дополнительно улучшить применение метаданных с использованием типов содержимого. Организации могут использовать типы содержимого для стандартизации конкретных типов файлов, документов или элементов списка. В рамках этих типов содержимого они могут включать требования к метаданным, шаблоны документов, настройки хранения и рабочие процессы напрямую. Это важно для получения лучшего опыта работы с поисковой службой.

Управление типами содержимого

Организации могут использовать типы содержимого для оптимизации работы своих пользователей в SharePoint 2016. Вы можете создавать шаблоны для определенных типов файлов, документов или элементов и включать метаданные с типом контента. Таким образом, вы можете повторно использовать тип содержимого на многочисленных сайтах, списках или библиотеках в иерархии SharePoint 2016. Тип содержимого становится стандартной ссылкой для типа информации, которую вы храните.

Многие организации имеют стандартные документы или стандартные требования к информации, которые часто повторяются. Типы содержимого позволяют организациям указывать и контролировать стандарты, связанные с этой информацией.

Что такое таксономии?

В SharePoint 2016 организационная таксономия — это механизм классификации, который часто носит иерархический характер. Пользователи этой организации могут применять таксономию к документам или элементам, хранящимся в библиотеках или списках SharePoint.

Цель внедрения таксономии заключается в предоставлении средств для организации и классификации хранимого контента. Таксономии могут помочь пользователям:

- определить, как хранить информацию;
- знать, где найти информацию;
- определить целевую аудиторию информации;
- определить цель информации.

Когда вы планируете таксономию, вы должны учитывать, как и почему пользователи могут захотеть классифицировать или организовывать контент.

Общие таксономии включают следующие типовые классификации:

- География, такая как страна, регион, месторасположение офиса или сайт.
- Конфиденциальность, например, государственная, частная, конфиденциальная или секретная.
- Отделы, такие как человеческие ресурсы, ИТ, производство или логистика.
- Проекты или программы.
- Внешние таксономии, такие как поставщики или клиенты.

Организации также могут создавать «народную классификацию» (фолксономию) с помощью функции Enterprise Keywords в SharePoint 2016. Фолксономия — это более гибкий способ организации или категоризации содержимого, который пользователи могут добавить без участия администратора.

Пользовательские столбцы и столбцы сайта

В SharePoint 2016 вы можете создавать собственные столбцы для хранения информации, такой как метаданные или данные элемента. При создании настраиваемых столбцов вы можете выбрать тип данных для столбца и указать информацию, хранящуюся в столбце.

Типы данных столбцов включают:

- текст или HTML-контент;
- предопределенный список вариантов или вариантов, основанных на другом списке на сайте;
- числа;
- валютные значения;
- записи даты и времени;
- пользователь или группа, выбранная из SharePoint или доменных служб Active Directory (AD DS);
- гиперссылка или изображение;
- вычисляемое значение, основанное на значениях других столбцов;
- выбор из набора управляемых метаданных.

Вы можете создавать столбцы в определенном списке или библиотеке. Однако эти столбцы доступны только для элементов в этом списке или библиотеке, и вы не можете использовать их в других списках или библиотеках.

Вы также можете создавать столбцы сайтов, которые затем могут быть связаны с любым списком или библиотекой на уровне или ниже этого сайта в пределах той же коллекции сайтов. Создание столбца сайта на сайте верхнего уровня коллекции сайтов означает, что этот столбец можно использовать в любом месте коллекции сайтов.

Вы должны использовать столбцы сайта при добавлении свойств метаданных к типам содержимого.

Что такое типы содержимого?

Типы содержимого — это мощный метод для создания содержимого определенного типа и автоматического связывания столбцов, метаданных, шаблонов документов, политик управления информацией и рабочих процессов с этим типом элемента.

Например, рассмотрим сценарий, в котором организация выполняет множество проектов, и для каждого проекта требуется конкретный бизнес-кейс. У организации уже есть шаблоны Microsoft Word, который могут использовать руководители проектов, но организация хочет оптимизировать процессы и определить, кто обновляет документ бизнес-кейса. В этом примере вы можете создать тип содержимого бизнес-кейса. Тип контента будет включать в себя шаблон документа, и вы можете включать любые требования к метаданным, такие как перечисление кода проекта и менеджера проектов, в качестве настраиваемых столбцов. Вы можете реализовать аудит для бизнес-кейса с помощью политики управления информацией в типе содержимого, и вы можете приложить рабочий процесс к типу содержимого для целей проверки и уведомления.

Все типы содержимого, которые вы создаете, должны иметь тип родительского содержимого. Тип родительского содержимого определяет, является ли тип содержимого, который вы создаете, типом списка или типа библиотеки. Кроме того, тип дочернего содержимого наследует столбцы и другие параметры из родительского типа содержимого.

Обзор управляемых метаданных

Метаданные — это информация о файлах или документах. Например, метаданные для документа могут содержать информацию об авторе документа или дату последнего изменения документа. В SharePoint 2016 вы можете управлять метаданными различными способами и стандартизировать свои метаданные на разных сайтах, коллекциях сайтов, веб-приложениях и фермах для создания таксономий или народных классификаций, которые помогают пользователям более эффективно определять и использовать контент.

Метаданные могут предоставить следующие преимущества:

- Вы можете использовать метаданные для предоставления дополнительных ссылок или контекста для элемента или файла, и пользователям не нужно открывать элемент, чтобы просмотреть эту информацию.

• Вы можете использовать метаданные для категоризации информации. Это полезно, если вы хотите фильтровать представления и отображать только соответствующую информацию.

• Вы можете искать содержимое через метаданные или ключевые слова. Метаданные индексируются и доступны для поиска, и вы можете использовать страницу результатов поиска для фильтрации результатов поиска по значениям метаданных.

• Вы можете использовать метаданные, чтобы обеспечить структуру навигации для сайтов и упростить отображаемый URL-адрес ключевых страниц.

Пользователи могут отмечать элементы с помощью ключевых слов предприятия, чтобы помочь с поиском. Ключевые слова предприятия хранятся как единый, плоский список ключевых слов, которые все пользователи могут использовать и обновлять. Ключевые слова предприятия могут участвовать в народной классификации для содержимого внутри организации.

Если вы предпочитаете более контролируемое использование метаданных, вы можете использовать термины. Термины — это плоские или иерархические списки текстовых записей, которые можно использовать в качестве метаданных в столбцах SharePoint. Например, вы можете использовать термины для создания категорий или классификаций для документов. Список терминов часто закрыт для редактирования, поэтому только назначенные пользователи могут обновлять список, тем самым обеспечивая контролируемую таксономию.

Вы также можете использовать термины в качестве элементов навигации на сайтах быстрого запуска (текущая навигация) или верхней ссылки (глобальной навигации). Это называется управляемой навигацией и обычно подразумевает использование каталога продуктов и веб-частей, основанных на поиске.

> *Примечание. Вы должны различать термины и ключевые слова. Как правило, администраторы предопределяют термины, тогда как ключевые слова часто не предопределены. Администраторы могут преобразовать ключевые слова в термины, используя «инструмент управления магазином терминов».*

Вы можете создавать типы содержимого для представления определенных типов файлов или документов, например, проектного предложения или документа бизнес-процесса. Типы содержимого могут иметь определенный шаблон документа, а также набор определенных столбцов для метаданных. Вы можете создавать типы содержимого в коллекции сайтов для использования только в той же коллекции сайтов, или публиковать коллекцию сайтов как концентратор типа содержимого, чтобы типы содержимого могли использоваться во многих коллекциях сайтов.

SharePoint 2016 предоставляет управляемые метаданные в виде терминов, наборов терминов, групп терминов и владельцев набора сроков. Следующий список объясняет эту терминологию:

• **Термин**. Термин — это индивидуальное значение или запись, которую вы хотите предоставить пользователям, которые они могут использовать в качестве метаданных. Например, термин может быть отдельным офисом или индивидуальным идентификационным кодом для проекта.

• **Набор терминов**. Набор терминов представляет собой список связанных терминов. Например, набор терминов может быть списком офисов организации или списком всех идентификационных кодов проекта. Набор терминов может предоставлять собой плоский список или иерархический список. Вы можете использовать набор терминов в качестве типа столбца управляемых метаданных.

• **Группа терминов**. Группа терминов представляет собой коллекцию наборов терминов, которой может быть сопоставлен набор разрешений доступа. Вы можете планировать группы терминов на основе пользователей, которым необходимо обновлять, изменять или исключать термины в наборах терминов. В SharePoint 2016 группы терминов могут быть локальными или глобальными.

• **Менеджер группы терминов**. Менеджер группы терминов может вносить изменения в набор терминов, например, добавлять новые термины, исключать термины или изменять разрешения для других пользователей в наборе терминов.

• **Участник**. Участник может вносить изменения в термины и термины в пределах группы терминов, но не может изменять разрешения для группы терминов.