

ПОСТРОЕНИЕ СИСТЕМЫ ХРАНЕНИЯ ДАННЫХ НА NAS-СЕРВЕРАХ: СТРАТЕГИЯ РАЗВИТИЯ

Варламов Николай Евгеньевич

руководитель отдела сервисно-технической поддержки,
SLMP PTE Ltd. коммерческо-маркетинговый представитель
Synology Inc. в России и СНГ

Статья «Храни меня, мой СХД», опубликованная авторами в № 3 журнала «Алгоритм безопасности», была посвящена организации системы хранения данных (СХД) на примере промышленного предприятия: что хранить, где хранить, как хранить и какие службы обеспечивают хранение. Данная статья знакомит читателей с примером организации системы хранения данных на NAS-серверах и включающую систему видеонаблюдения.

Каждая крупная или даже средняя компания имеет, как правило, четкую стратегию формирования своей ИТ-инфраструктуры и сложившийся парк компьютерного оборудования. Можно утверждать, что поступательный рост компании будет рождать проблемы, связанные с оперативным введением в работу все новых и новых технических ресурсов. Одним из наиболее острых технических вопросов является расширение возможностей всей ИТ-системы предприятия по сохранению и распределению интенсивно вырабатываемых объемов данных. Несмотря на то, что наиболее «горячие» вопросы обеспечения ресурсами хранения данных чаще всего возникают на каких-то четко ограниченных функциональных участках, они требуют такого же немедленного реагирования, как и вопросы, относящиеся к основным серверам компании. Именно для таких задач предлагаются решения, ориентированные на обеспечение решения локальных задач для крупных предприятий и общекорпоративных — для средних.

Суть решения заключается в замещении традиционных файловых серверов на основе ПК-платформы специализированными сетевыми устройствами хранения данных NAS.

Замещение не означает отказ от использования имеющегося парка серверного оборудования. Данное решение подразумевает его расширение при возникновении дополнительных задач за счет оперативного введения в строй не новых дорогостоящих серверов, а именно NAS-хранилищ. По своим функциональным ролям эти устройства могут выступать в качестве общекорпоративного

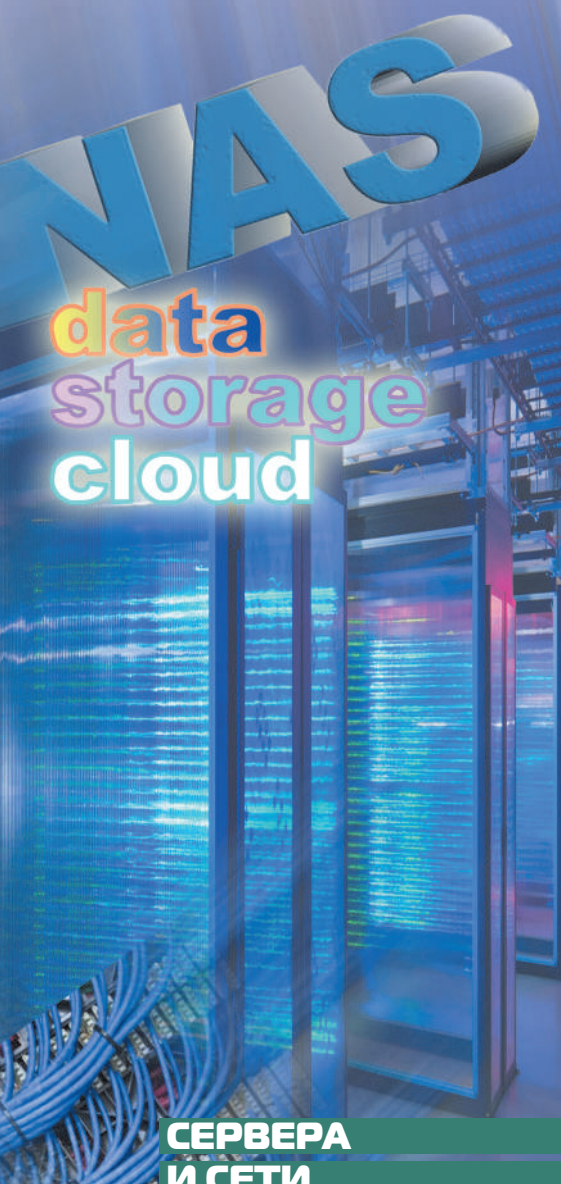
файл-сервера, выделенного сервера отдела или департамента, сервера для хранения резервных копий с обрабатывающих серверов или основных файловых Windows или Linux-серверов предприятия. Применение именно NAS, а не традиционных ПК-серверов позволит ввести в работу новую дисковую емкость практически моментально, серьезно сэкономить на приобретении аппаратной платформы и, что иногда более затратно, на покупке серверных лицензий.

Рассмотрим схему применения сетевых накопителей в среднем предприятии как эталонный пример инсталляции (рис. 1).

Порядок работы изображенной структуры: предположим, что компания имеет домен, контроллером которого является Windows-сервер, и выработаны централизованные типовые политики разделения доступа к ресурсам домена для каждого типа групп. В компании существуют группы: менеджеры, руководство и бухгалтерия, плюс к этому существует удаленная группа в филиале, которая входит в домен через VPN-соединение.

Каждая основная функционально разная пользовательская группа предприятия получает в свое распоряжение выделенный сервер хранения данных на основе NAS:

1. Мощные дисковые сетевые накопители, исполняющие роль хранения общего рабочего архива предприятия. NAS работает в режиме массива RAID5 или RAID6 с подключением к сетевому многопортовому коммутатору через 2 LAN-порта Gigabit Ethernet с агрегацией каналов. На нем хранится весь массив файлов, постоянно требуемый в общем пользовании для всех сотрудников, не зависимо от того,



**СЕРВЕРА
И СЕТИ**

к какому департаменту они относятся. Это могут быть коллекции дистрибутивов программного обеспечения, банк фотографий продукции, банк несекретной технической документации. Кроме того, на этом же ресурсе могут находиться изолированные от общего доступа личные дисковые квоты каждого пользователя, на которых они обязаны размещать важные рабочие документы, создаваемые на локальных ПК. Сервера могут хранить образ рабочих ПК полностью — с системой и данными, — что позволяет, в дальнейшем, перенести рабочий ПК на другую аппаратную платформу, в том числе и в виртуальную среду. В зависимости от программного обеспечения системы хранения, размещение копий рабочих документов с локальных ПК сотрудников можно перевести и автоматический режим. Проведя настройки удаленно или локально, администратор домена сможет гарантировать сохранность данных со всех ПК сети при случайной или умышленной утрате файлов. Резервирование может производиться абсолютно автономно по предзаданному расписанию.

2. Высокопроизводительные дисковые сетевые накопители выполняют роль сервера, на который производят резервирование главные сервера компании: такие как основной файл-сервер, SQL-сервер (при необходимости) и т.д., и, если того требуют обстоятельства, контроллер домена (резервирование базы Active Directory, журналы событий и пр.). На этот же NAS производит резервирование в автоматическом режиме через VPN-канал файл-сервера филиала/филиалов компании. Также на накопитель 2 может производить резервирование основное файловое хранилище 1. Резервирование с WAN и LAN-ресурсов в порядке борьбы с хакерами и инсайдерами может производиться в режиме защищенного канала. Основное серверное оборудование будет по-прежнему иметь централизованное размещение в специально отведенном месте с выполнением условий ограничения к нему физического доступа и заданных климатических требований.

Решая вопрос о подборе сервера, на который осуществляется резервирование основных серверов компании, необходимо отметить два важных требования надежности к нему: возможность горячей замены и жестких дисков, и блоков питания.

Выполнение этих условий обеспечивает гарантированную защищенность сервера резервирования от неожиданного выхода из эксплуатации. Если же выбранный накопитель имеет в наличии два сетевых интерфейса Gigabit Ethernet, это позволяет обеспечить быстрый канал связи с другими серверами в режиме агрегации каналов или перехватывающего дублирования каналов при повышенных требованиях к устойчивости соединения.

Мы намеренно не разделяем в схеме физически устройства, отвечающие за выполнение задач 1 и 2, — все они объединены программным приложением виртуализации. Это продукт, который позволяет строить виртуальную среду предприятия. Речь идет о том, что благодаря достаточно высокопроизводительным системам хранения данных с мощными процессорами Intel Xeon заказчик сможет отказываться от отдельных физических серверов, используя вычислительные мощности и дисковое пространство СХД для виртуальных приложений. Объединяя СХД в кластеры, можно строить конвергентную архитектуру, где каждый физический элемент одновременно представляет собой и СХД для хранения данных, и вычислительный узел для их обработки, и в задачу программного обеспечения будет входить бесперебойная работа созданной виртуальной среды, что достигается использованием различных технологий высокой доступности, репликации и миграции. В случае сбоя или при необходимости, виртуальные машины могут просто переноситься с одного узла на другой, а доступ к данным всей инфраструктуры сохранится даже при остановке одного или даже двух ее физических узлов. Создание конвергентных систем, где нет разделения на узлы хранения и узлы вычисления, — не такая уж и новинка, подобные решения есть у производителей СХД корпоративного класса, но стоимость этих решений не сопоставима с тем, что предлагают производители NAS-серверов.

Важно, что приложения для виртуализации совместимы даже с настольными NAS-ми, причем и не только с топовыми на 36 дисков, но и с простейшими. Таким образом, конвергентная виртуальная архитектура возможна не только для крупных предприятий, но и та же самая виртуальная платформа может быть установлена на коробочку с одним процессором Celeron и потребляемой мощностью около 20 Вт. Для компаний-производителей NAS-серверов отправной точкой стали малые офисы на 10–20 сотрудников. Впоследствии, с ростом потребностей офисов, заказчик сможет расширить свою IT-инфраструктуру за счет замены NAS-ов на более производительные. И вот эта возможность — начать с копеечной виртуальной среды и расширяться по мере роста потребностей — и есть та самая стратегия роста, которая применима не только к банкам или фармакологическим компаниям, не стесненным в средствах, но и к небольшим организациям, которые начинают с того, что переносят несколько Windows или Linux-приложений на одну физическую коробочку, а потом по мере роста бизнеса эту коробочку меняют, оставаясь в комфортной и привычной виртуальной среде.

3. Высокоскоростной двухдисковый сетевой накопитель выполняет роль индивидуального сервера для руководящего состава. Накопитель 3 может централизованно управляться администратором сети и осуществлять резервирование на центральные back-up сервера 2. Устройство 3 обеспечивает руководителя личным, отделенным (в том числе и физически) от ресурсов общего пользования объемом хранения, который пополнит скромные емкости встроеного жесткого диска ноутбука. Подключение может иметь как проводной, так и беспроводной канал, что в совокупности со скрытым размещением, возможным благодаря скромным размерам накопителя 3, дает дополнительную степень безопасности. В силу специфики работы руководства преимущественно с данными текстового и мелко-графического типа двухдисковый накопитель может стать необходимым и достаточным выбором по соотношению цена/объем/возможности.

4. Данные накопители выполняют функцию локальных мини-серверов, обеспечивающих узко-специфицированные задачи хранения. Они могут быть предназначены для целей хранения бухгалтерской базы (допустим, базы 1С) — для бухгалтерии, технической документации — для отделов разработки или продаж, персональных данных сотрудников — для кадровой службы и т.д., что по своей сути зачастую требует изолирования от ресурсов общего пользования. Кроме того, ввиду высоких требований к надежности хранения ответственных данных, выбирается сетевой накопитель, оптимальный по соотношению: возможность зеркалирования дисков/достаточная емкость/умеренная стоимость. В описываемой модели использования накопителя 4 работают только как выделенное устройство хранения самой определенной базы, обработкой запросов к этой базе и ее модификацией занимается обрабатывающий сервер: в данном случае подразумевается выделенный SQL-сервер. На этом же NAS могут держать свои рабочие документы высокой секретности и сотрудники отдела. Дополнительным требованием при выборе этого накопителя является высокая скорость функционирования, обеспечивающая нормальный поток обмена данными с рабочей группой и обрабатывающим сервером.

5. Аналогичный накопителю 4 используется в описываемой модели в качестве основного сервера филиала. Возможность организации хранения на нем достаточного объема данных, максимальная простота первичной настройки и отсутствие необходимости последующего обслуживания — решающие аргументы в выборе оптимального решения для обеспечения средствами хранения удаленных офисов. Кроме того, поставив в

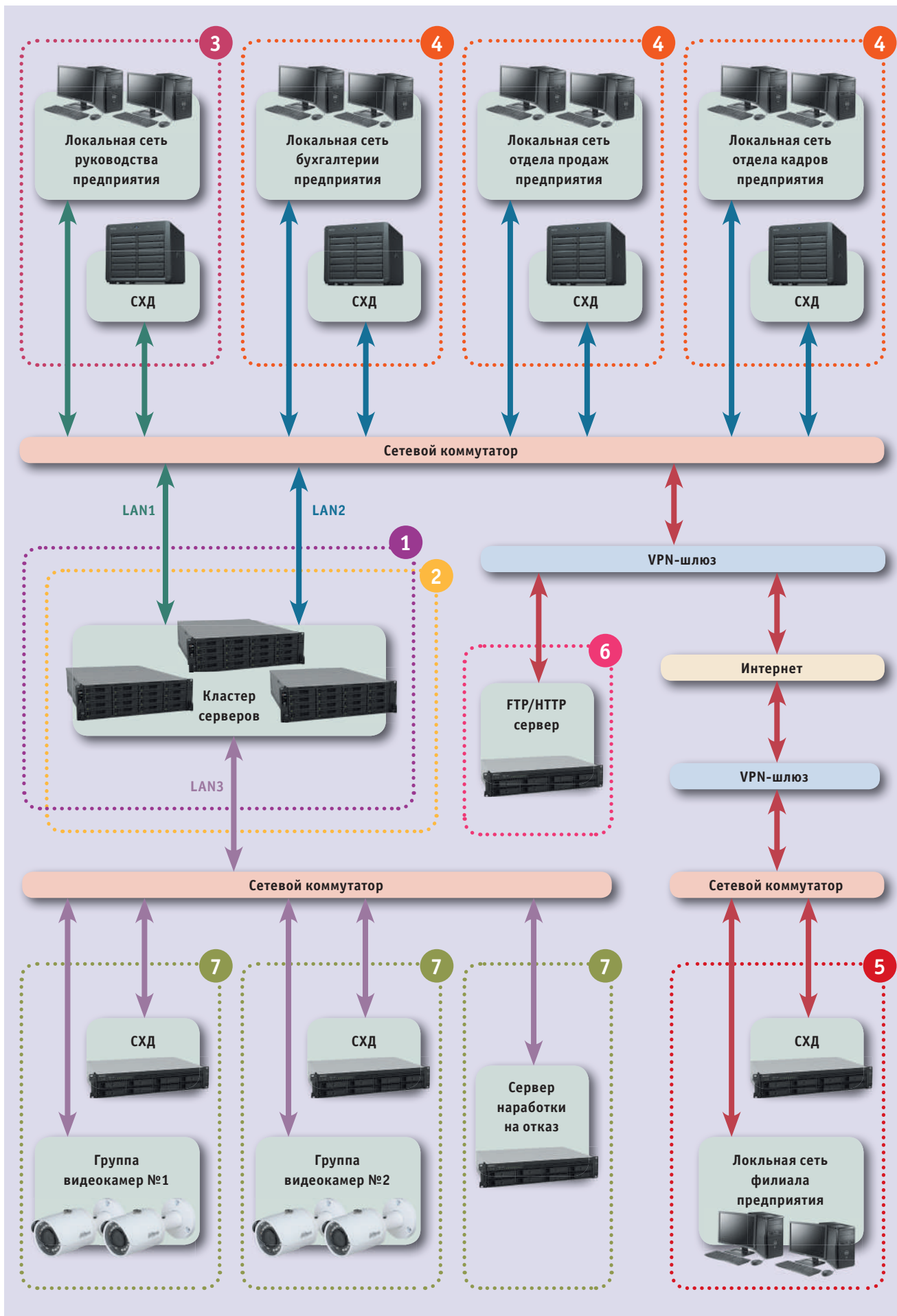


Рис. 1. Схема применения сетевых накопителей в среднем предприятии

филиал или дополнительный офис накопитель 4, вы автоматически решите вопрос совместного доступа к принтерам, контрольного видеонаблюдения, FTP-обмена файлами и построения локального веб-ресурса. При объединении через VPN-соединение локальной сети филиала с сетью головного офиса вопрос резервирования рабочего массива данных филиала и репликации учетных баз филиала на центральные серверы хранения решается автоматически. В условиях наличия удаленных офисов и филиалов с ограниченным числом сотрудников вопрос надежности хранилища данных, скорости и простоты его первичного развертывания, а также последующей эксплуатации с возможностью удаленного администрирования выходит на первый план.

6. Двухдисковый сетевой накопитель начального уровня, обеспечивающий задачи обмена данными с внешними пользователями и партнерами компании. Находясь вне домена компании за маршрутизатором в DMZ-зоне, накопитель 6 является внешним файлообменным ресурсом компании для передачи файлов большого объема через Интернет. При таком решении по размещению сетевого накопителя вне зоны домена решается одна из ключевых задач безопасности — исключение проникновения внешнего потока запросов и данных внутрь зоны домена.

Работа с данным ресурсом осуществляется в следующем порядке: администратор создает список пользователей внутренней сети, имеющих доступ к накопителю 6 по протоколам NFS или Samba, для добавления или удаления требуемых к публикации файлов. После этого добавляются учетные записи типовых или специфицированных по уровню доступа пользователей для доступа из Интернета по протоколу FTP. Доступ по FTP к серверу 6 возможен и для пользователей внутренней сети. Кроме работы с сервером 6 как с FTP-ресурсом, возможно использование его как мини веб-сервера для каких-либо узких целевых задач, например, публикации на web открытых для определенного круга партнеров или сотрудников филиала технических документов, изображений товара, прайс-листов и пр. Возможно и дублирование доступа через HTTP к тому, что опубликовано для FTP-доступа.

Еще одной функцией, которую можно возложить на накопитель 6, является автономное получение контента из внешних сетевых ресурсов, таких как http-сайты, ftp-сервера и даже BitTorrent-сети. Чрезвычайно много служебных системных обновлений для используемого оборудования, программного обеспечения, графических и видеообъектов, да и любых других типов данных находится в свободном доступе в web, имея при этом не

маленькие объемы. Во избежание лишней нагрузки на рабочий ПК администратора и пользователей можно перепоручить задачу скачивания большого по объему контента сетевому накопителю.

Ввиду средней нерегулярной нагрузки на данный функциональный узел использование двухдискового начального уровня мощности накопителя является необходимым и достаточным выбором.

Учитывая, что данная публикация адресована, в первую очередь, рынку систем безопасности, обозначим место серверов системы видеонаблюдения в приведенной структуре. Выбор подсистемы не случаен: с одной стороны, нормативная база предписывает большому числу типов предприятий этой подсистемы, а с другой стороны, ни одна другая система не нагружает так хранилища и локальные вычислительные сети, как система видеонаблюдения.

7. В идеале, если система видеонаблюдения разветвленная, каждой группе камер выделяется свой NAS-сервер, а также общий для системы резервный FServer для отработки отказа сервера/-ов записи, с установленной на нем программной частью системы видеонаблюдения. Через коммутаторы к серверам предприятия проложена от хранилищ системы видеонаблюдения, выделенная ЛВС. Эти меры позволяют системе безопасности работать с данными системы видеонаблюдения на своей части сети. Данные системы и ее вычислительные мощности надежно укрыты от внешнего (по отношению к системе хранения предприятия) и внутреннего (сотрудники подразделений предприятия, не наделенные правом доступа к данным системы видеонаблюдения) воздействия.

РЕЗЮМЕ ПО ПРЕДСТАВЛЕННОМУ РЕШЕНИЮ

Описанное решение является примером частично децентрализованной модели использования системы хранения данных. То есть, мы подразумеваем, что в системе остается основной сервер хранения данных для задач, требующих высочайшей производительности, и контроллер домена, определяющий политику. Однако все расширение системы произведено за счет введения на отдельные функциональные участки выделенных NAS-хранилищ.

В результате использования такой модели предприятие, разгружая от постоянной массовой нагрузки уже имеющийся основной сервер, продолжает работу с ним на конкретных высоконагруженных секторах сети. И для этого его производительности по-прежнему хватает. Таким образом, происходит сохранение ранее произведенных бюджетных вложений в IT-инфраструктуру. Дальнейшее масшта-

бирование и наращивание возможностей по хранению данных происходит за счет введения в эксплуатацию сетевых многодисковых накопителей, приобретение которых производится по мере возникновения конкретных оперативных функциональных задач.

С точки зрения пользователей, такая модель не будет существенно отличаться от централизованной модели, так как все их потребности по хранению и общему доступу будут с успехом покрываться. Одновременно такая модель приносит ряд существенных плюсов, таких как распределенность нагрузки на ресурсы за счет их множественности и исключение выхода из строя сразу всего массива хранения ввиду этой же причины.

Весьма вероятен выход из строя даже самого отказоустойчивого дискового массива сверхвысокой емкости за счет отказа не самих единиц хранения (дисков), а платформы или ее ключевых элементов. Но достаточно трудно представить себе случай, когда одновременно выйдут из строя сразу все (или даже большая часть) отдельных сетевых накопителей, обладающих идентичной централизованному мега-хранилищу совокупной емкостью.

Тем более, при использовании того же централизованного сверхвысокоемкого массива в компании, имеющей несколько рабочих групп (отделов) с различными функциональными задачами, как правило, неизбежно логическое разделение совокупной емкости на отдельные изолированные по принципу деления прав доступа дисковые квоты. Вычислительный же ресурс сервера хранения, обеспечивающий обслуживание групп по мере их роста, даже в случае возможности наращивания массива хранения, будет оставаться на одном и том же уровне, что будет приводить к торможению в обслуживании.

Сопоставляя затраты на построение централизованной системы хранения данных для задач среднего бизнеса с аналогичной задачей, реализуемой через постепенное масштабирование отдельными сетевыми накопителями, можно обнаружить очевидный бюджетный выигрыш в пользу NAS-решений как на стадии закупок оборудования, так и на стадии их последующей эксплуатации. Более того, в отдельных случаях даже крупные корпорации могут с успехом решать локальные (особенно требующие экстренного решения) задачи хранения данных для департаментов и отдельных рабочих групп оперативным введением в эксплуатацию сетевых накопителей средних и старших моделей.

Использование NAS гарантирует предприятию одновременно и масштабируемость, и надежность, и экономическую выгоду при очень высоком удобстве эксплуатации.