

Техническая проверка:

Защита данных с помощью решения корпоративного класса **InfiniGuard** от **Infinidat**

Уверенное восстановление критически важных для
бизнеса рабочих нагрузок

Винни Чоински, старший аналитик по проверке; Брайан Гарретт, исполнительный
вице-президент по услугам проверки
Май 2021 г.

Настоящий отчет “Техническая проверка” был подготовлен по заказу Infinidat компанией ESG и
распространяется по лицензии ESG.

Содержание

Введение	3
Преамбула	3
Обзор решения InfiniGuard	4
Техническая проверка ESG	5
Реальная производительность при восстановлении	5
Архитектурные особенности	8
Управление системой и интеграция для защиты данных	9
Резюме	13
Приложение	14

Технические проверки ESG

Цель технических проверок, проводимых компанией ESG, – дать ИТ-специалистам знания о решениях в области ИТ, пригодных для компаний любого типа и размера. Технические проверки ESG призваны не заменить собой процесс оценки, которую следует проводить перед принятием решения о покупке, а, скорее, дать представление об этих новых технологиях. Наши цели состоят в том, чтобы изучить отдельные наиболее ценные особенности и функции ИТ-решений, показать, как их можно использовать для устранения реальных проблем заказчиков, а также выявить области, требующие улучшения. Мнение экспертов из проверочной команды ESG о сторонних продуктах основано на практическом тестировании, которое проводим мы сами, и наших интервью с заказчиками, которые используют эти продукты в продуктивных средах.

Введение

В настоящем отчете описано проверочное тестирование решения Infinidat InfiniGuard для защиты и восстановления данных, проведенное компанией ESG для изучения преимуществ архитектуры InfiniGuard (включая использование неизменяемых моментальных снимков для восстановления после атак программ-вымогателей, высокую производительность резервного копирования и восстановления при оптимальной стоимости, а также простоту развертывания и управления).

Преамбула

Поскольку информационные технологии уже стали неотъемлемой частью современного бизнеса, простои ИТ-систем влияют на всю компанию, а не только на ее ИТ-отдел. Астрономические потери, вызванные простоями ИТ-систем (будь то из-за успешной кибератаки или сбоя самой системы) широко освещаются, а убытки из-за одного такого инцидента часто измеряются миллионами долларов. Но гораздо хуже задокументированы другие аспекты влияния простоев критически важных приложений на бизнес.

Согласно исследованию рынка, проведенному компанией ESG, современные организации рассматривают простои ИТ-систем минимум с двух разных точек зрения: времени и бизнес-факторов (таких как упущенная выручка или сниженная производительность труда). С точки зрения времени длительность перерыва в работе ИТ-систем имеет критические последствия для бизнеса. Как показывает практика, для большинства организаций один час простоя – это очень много. 15% опрошенных компаний ESG заявили, что для их организаций простои критически важных приложений недопустимы практически *никогда*. Более половины (57%) сообщили, что для них недопустим часовой перерыв в работе этих ключевых приложений.¹

Если же говорить о бизнес-факторах, то простои ИТ-систем влияют на организации по-разному. На Рис. 1 показаны последствия, которые, по мнению организаций, могут повлечь простой в работе приложений или потерю данных. На первый взгляд может показаться удивительным, что респонденты намного чаще говорили о потере производительности труда работников, чем о потере выручки компании или ухудшении репутации бренда.

Однако, следует помнить, что, например, в больницах, коммунальных предприятиях, организациях сферы обслуживания и так далее, зарплаты продолжают начисляться, а расходы – расти, даже когда персонал бездействует из-за простоя. Фактически для многих организаций работники настолько важны, что о потере их доверия респонденты говорили чаще, чем о потере выручки.²

Рис. 1. Пять основных типов влияния простоя или потери данных



Источник: Enterprise Strategy Group

¹ Источник: Исследовательский отчет ESG, [Соглашения об уровне обслуживания и требования к доступности в реальной жизни](#), Октябрь 2020 г.

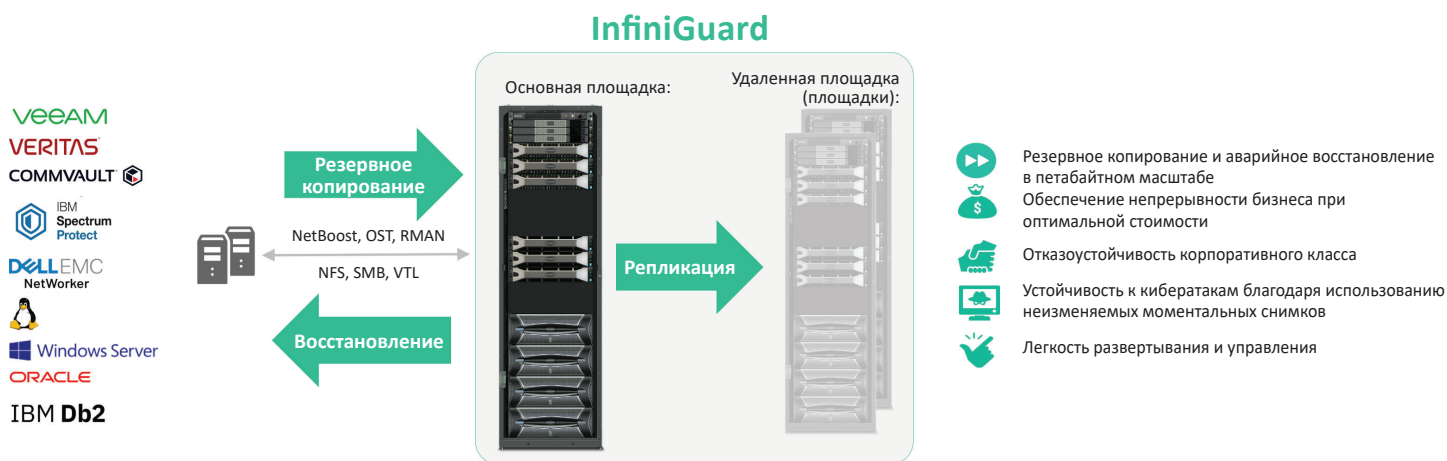
² Источник тот же.

Обзор решения InfiniGuard

InfiniGuard — это петабайтное решение для резервного копирования, восстановления данных и аварийного восстановления, которое снижает затраты, риски и время простоя, связанные с восстановлением критически важных для бизнеса прикладных рабочих нагрузок после кибератаки, сбоя оборудования, стихийного бедствия или случайного повреждения данных.

Как показано на Рис. 2, лучшие в отрасли приложения резервного копирования и базы данных (например, Veeam, Veritas, Commvault, IBM Spectrum Protect, Oracle RAC, IBM Db2) при резервном копировании и восстановлении передают данные устройствам InfiniGuard и от них по сети Ethernet или Fibre Channel при помощи стандартных отраслевых протоколов (NFS, SMB, VTL, NetBackup OST, Veeam Data Mover и Oracle RMAN). Дедуплицированные данные, позволяющие эффективно использовать емкость хранилищ, шифруются и реплицируются по сетевому подключению с основной площадки на одну или несколько удаленных площадок для аварийного восстановления.

Рис. 2. Обзор решения InfiniGuard



Источник: Enterprise Strategy Group

Основные возможности и функции:

- Высокоэффективная защита данных корпоративного класса со скоростью резервного копирования до 115 ТБ/час, позволяющая заказчикам соблюдать все более строгие требования современных предприятий по уровням обслуживания.
- Оптимизированное по стоимости обеспечение непрерывности бизнеса за счет сочетания технологий, включая интеллектуальное кэширование и сокращение объема данных.
- Отказоустойчивость корпоративного класса на основе аппаратного резервирования по схеме N+2, которое гарантирует, что сервисы защиты данных продолжают работать после нескольких одновременных отказов оборудования или носителей (например, резервирование контроллеров по схеме N+2, резервирование дисков InfiniRaid со средним временем пересборки (ребилда) носителей 15 минут после отказа двух дисков).
- Использование неизменяемых моментальных снимков для быстрого и безопасного восстановления одной или нескольких прикладных рабочих нагрузок после кибератаки (например, программы-вымогателя).
- Легкость развертывания и управления благодаря функциональной совместимости (Plug and Play) с популярными корпоративными приложениями резервного копирования и базами данных. Чтобы начать работу с InfiniGuard, достаточно в параметрах конфигурации существующего приложения резервного копирования в качестве места хранения данных резервного копирования задать новый том InfiniGuard.

Техническая проверка ESG

Компания ESG проверила возможности и полезность решения InfiniGuard для резервного копирования и аварийного восстановления, проведя ряд демонстраций, сеансов удаленного тестирования, проверок производительности и бесед с заказчиками. В остальной части этого отчета исследуются преимущества архитектуры InfiniGuard, включая использование неизменяемых моментальных снимков для восстановления после атак программ-вымогателей, высокую производительность при оптимизированной стоимости, а также простоту развертывания и управления.

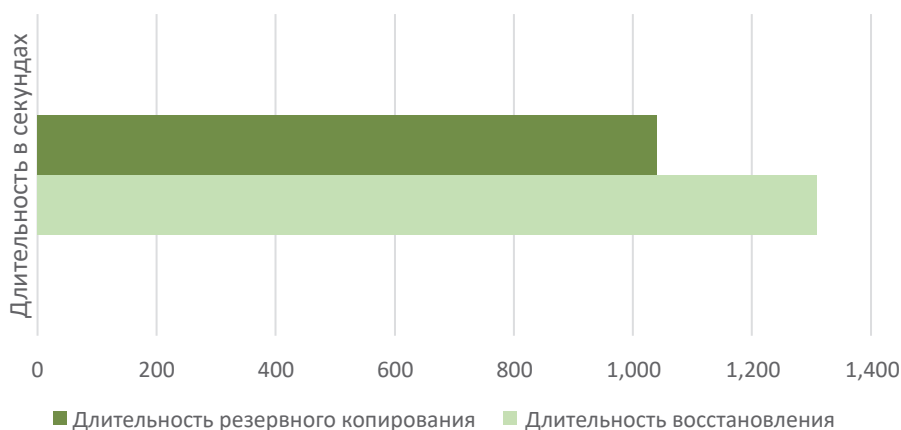
Реальная производительность при восстановлении

Производительность всегда была важной чертой любого хорошего решения корпоративного класса для защиты данных. Однако многие из последних нововведений в этой области делали упор на передовых показателях производительности резервного копирования и эффективности использования дискового пространства, часто в ущерб возможности восстановления данных “в масштабе”. В этом разделе отчета мы рассмотрим некоторые реальные сценарии восстановления, позволяющие решению InfiniGuard защищать данные с эффективной емкостью до 50 ПБ и наращивать скорость резервного копирования до 115 ТБ/час при использовании протокола NetBoost.

В первом сценарии, показанном на Рис. 3, мы сравнивали производительность резервного копирования и производительность восстановления в лабораторной среде для рабочей нагрузки БД. Идея состояла в том, чтобы продемонстрировать способность InfiniGuard обеспечивать почти одинаковую производительность при резервном копировании и восстановлении. Здесь мы использовали сервер Linux, на котором работала двухтерабайтная БД Oracle с включенным сжатием по столбцам и прозрачным шифрованием данных. Мы сравнили первое полное резервное копирование с полным восстановлением БД на том же сервере Linux, подключенном по сети 10 GbE к общему дисковому сетевому ресурсу с поддержкой NetBoost на целевой системе InfiniGuard.

Рис. 3. Производительность при резервном копировании и восстановлении

Производительность при резервном копировании БД Oracle для защиты данных (резервное копирование и восстановление)



Источник: Enterprise Strategy Group

Что значат эти числа

- Исторически сложилось так, что полное восстановление обычно длится минимум на **50%** дольше полного резервного копирования. InfiniGuard перекрывает этот показатель и обеспечивает совсем небольшую разницу (**21%**) между длительностью полного резервного копирования и длительностью полного восстановления БД Oracle.
- 17 минут 20 секунд – столько длилось полное резервное копирование при использовании протокола NetBoost.

- 21 минута 50 секунд – столько длилось полное восстановление БД Oracle.
- Следует отметить, что при использовании протокола NetBoost даже первое полное резервное копирование выиграло от некоторой дедупликации на стороне клиента, включенной для повышения производительности. Поскольку индекс дедупликации в InfiniGuard строится после каждого нового резервного копирования, последующие операции защиты данных должны показать еще более высокую производительность.

Затем мы проанализировали и проверили продуктивную среду организации, развернувшей систему InfiniGuard. Заказчик работает в сфере доставки и логистики и использует конфигурацию с несколькими площадками (два активных ЦОД и один ЦОД аварийного восстановления). Заказчик перешел на InfiniGuard с клиент-серверного приложения резервного копирования, которое использовало комбинацию дисков и ленточных накопителей. Теперь он перешел в преимущественно виртуальную среду и использует Veeam и InfiniGuard для резервного копирования, восстановления работоспособности и аварийного восстановления. Это новое решение упростило инфраструктуру защиты данных и теперь позволяет заказчику извлекать пользу из улучшенной дедупликации и таких функций, как мгновенное восстановление. Несмотря на то, что заказчик использует как дедупликацию, так и неизменяемые моментальные снимки данных, он по-прежнему может использовать возможности мгновенного восстановления Veeam для восстановления серверов любого размера в этой среде за считанные минуты без заметного снижения производительности продуктивных систем. Как показано на Рис. 4, данные, полученные от множества заказчиков и проверенные компанией ESG, подтверждают, что это решение позволяет значительно уменьшить объем хранилища, необходимый для защиты. Данные системы поддержки Call Home были проверены и показали (на нашей выборке заказчиков) сокращение объемов данных до **31,8:1** при среднем значении **16:1**.

“Мы можем в нашей среде запустить мгновенное восстановление для серверов приложений любого размера из дедуплицированного хранилища InfiniGuard, и наши пользователи не заметят снижения производительности”.

Рис. 4. Эффективность СХД защиты данных



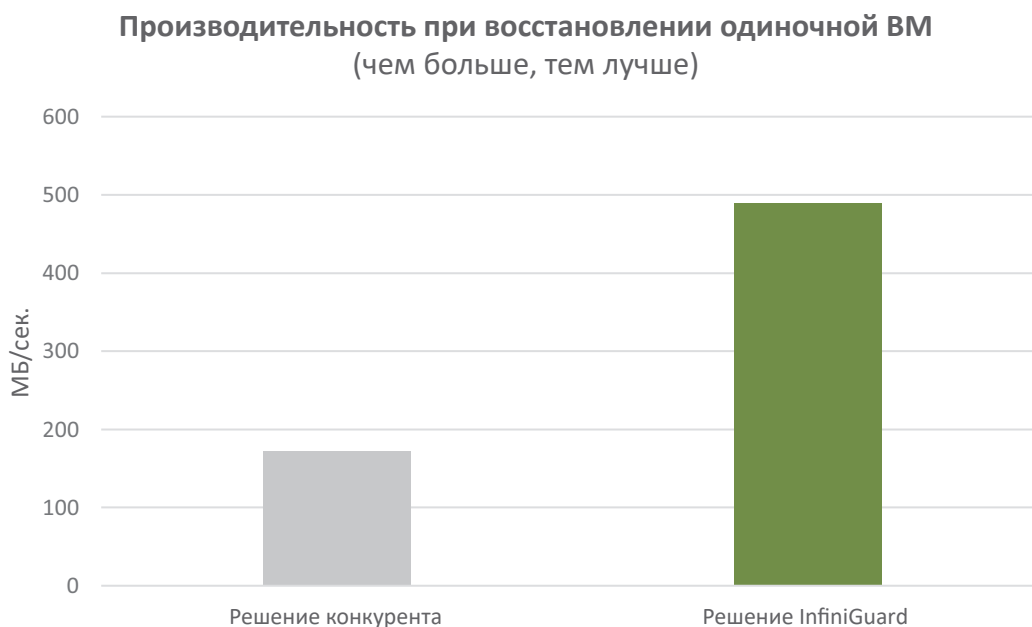
Источник: Enterprise Strategy Group

Что значат эти числа

- Благодаря дедупликации для защиты одного терабайта продуктивных данных с помощью InfiniGuard нужно было хранить в среднем лишь 60 ГБ данных.
- Сокращение объема данных с помощью InfiniGuard позволяет на **97%** уменьшить объем данных резервного копирования, который нужно хранить.

Наконец, мы проверили результаты текущего нагрузочного тестирования. Финансовая компания, специализирующаяся на образовательных услугах уровня колледжа, оценивала возможность заменить имевшиеся у нее специализированные устройства резервного копирования на систему InfiniGuard. Как показано на Рис. 5, мы сравнили пропускную способность, требуемую для восстановления одиночной продуктивной ВМ в один поток, с пропускной способностью InfiniGuard при восстановлении.

Рис. 5. Реальная производительность при восстановлении



Источник: Enterprise Strategy Group

Что значат эти числа

- Решение InfiniGuard обеспечило на **284%** более высокую пропускную способность, чем решение конкурента.
- ESG полагает, что при многопоточном восстановлении более крупных ВМ преимущество в пропускной способности InfiniGuard будет еще больше.



Почему это важно

Согласно исследованию ESG, более чем для половины опрошенных организаций часовой простой критически важных приложений недопустим. Организации также сообщили, что каждое третье приложение имеет важное значение для их бизнеса, что, в свою очередь, означает более строгие условия SLA. Согласно тому же исследованию, только двое из пяти опрошенных сообщили, что они всегда соблюдают свои соглашения SLA на восстановление.³

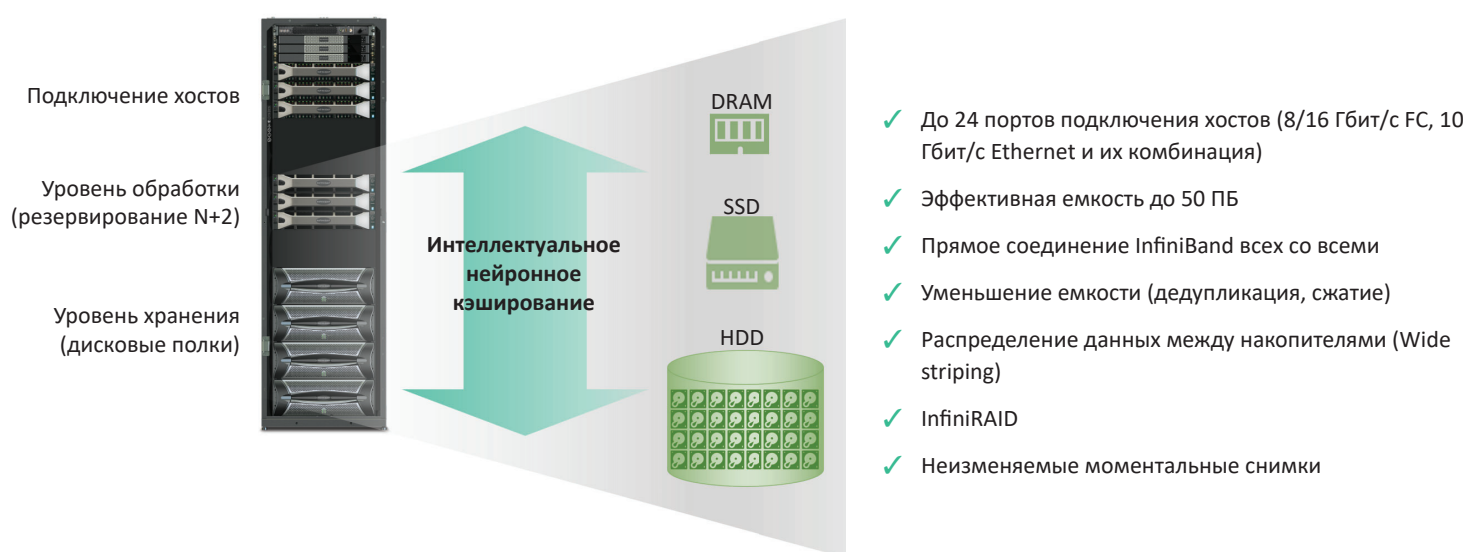
По мнению ESG, система InfiniGuard помогает решать проблемы производительности при защите данных в масштабе предприятия благодаря сочетанию высокопроизводительной СХД InfiniBox с технологией дедупликации корпоративного класса. Компания ESG подтвердила, что система InfiniGuard обеспечивает высокую производительность при восстановлении данных, необходимую для соблюдения соглашений SLA на восстановление.

³ Источник: Исследовательский отчет ESG, [Соглашения об уровне обслуживания и требования к доступности в реальной жизни](#), Октябрь 2020 г.

Архитектурные особенности

Общий обзор архитектуры специализированного устройства защиты данных InfiniGuard показан на Рис. 6. Приложения резервного копирования и серверы БД подключаются к СХД с эффективной емкостью до 50 петабайт, имеющей до 24 портов Fibre Channel и Ethernet. Для подключения хостов можно использовать разные комбинации сетевых транспортов и протоколов FC и Ethernet (например, NFS для серверов Unix, SMB для серверов Windows, а также специальные протоколы для ПО резервного копирования, такие как NetBackup OST и Veeam Data Mover).

Рис. 6. Архитектурные особенности



Источник: Enterprise Strategy Group

Интеллектуальное кэширование сочетает экономичность жестких дисков большой емкости для постоянного хранения данных с высокой скоростью относительно небольшого объема оперативной памяти DRAM и SSD (флеш-памяти) для кэширования. Сочетание недорогих жестких дисков (емкость) и интеллектуального кэша разумного объема (скорость) позволяет системе обеспечить производительность, близкую к производительности устройств резервного копирования полностью на твердотельных накопителях (all-flash), причем в разы дешевле систем all-flash.

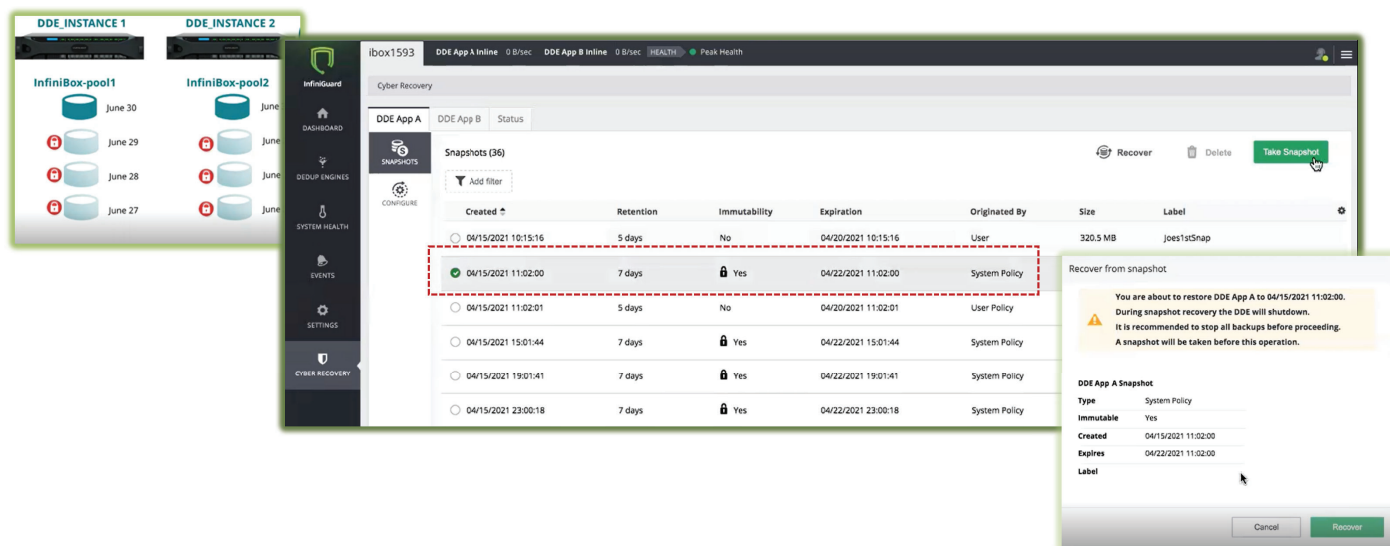
Прямое соединение InfiniBand всех со всеми создает высокоскоростной коммуникационный канал между уровнями подключения, обработки и хранения в архитектуре InfiniGuard. Любой узел хранения в кластере InfiniGuard может напрямую обращаться к памяти любого другого узла кластера посредством механизма прямого доступа к памяти (RDMA). Это снижает стоимость, сложность и паразитные задержки, свойственные специализированному устройству резервного копирования, в котором для внутренней связи используется коммутируемая сеть.

Уменьшение емкости обеспечивается алгоритмами дедупликации и сжатия, которые выполняются на стандартных серверах на уровне обработки. Дедупликация NetBoost на стороне источника (сейчас она поддерживается для целевых файловых систем общего назначения на серверах Linux и Windows, Veritas NetBackup OST, Oracle RMAN и IBM Db2) снижает сетевой трафик и увеличивает экономию за счет сокращения емкости.

Неизменяемые моментальные снимки и репликация позволяют создавать образы резервного копирования с однократной записью и многократным чтением (WORM) и сетевой изоляцией, что необходимо для безопасного и быстрого восстановления после кибератаки (например, программы-вымогателя).

На Рис. 7 показано, как можно использовать вкладку **CyberRecovery** в интерфейсе управления InfiniGuard для быстрого восстановления после атаки программы-вымогателя.

Рис. 7. Восстановление из неизменяемого моментального снимка



Источник: Enterprise Strategy Group



Почему это важно

Все больше и больше организаций пытаются обосновать необходимость затрат на обновление парка разнородных устаревших (и продолжающих устаревать) специализированных устройств резервного копирования до устройств all-flash последнего поколения, чтобы снизить риск потери данных после атаки программы-вымогателя и сократить (а то и вовсе исключить) простой критически важных для бизнеса приложений.

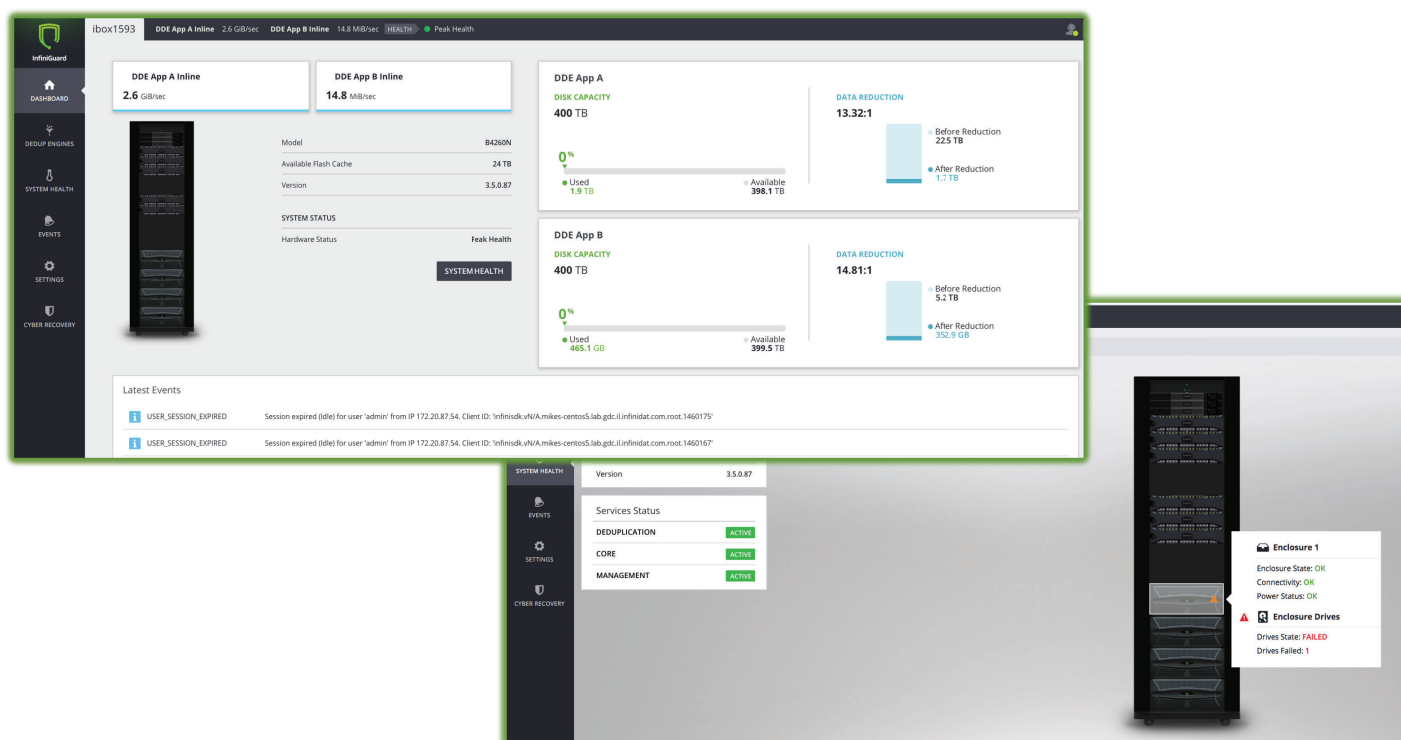
По мнению ESG, архитектура InfiniGuard идеально отвечает потребностям в резервном копировании и восстановлении единого набора ключевых бизнес-приложений в петабайтном масштабе после атак программ-вымогателей.

Управление системой и интеграция для защиты данных

Решением InfiniGuard легко управлять через интуитивно понятный графический пользовательский интерфейс на HTML5, который упрощает традиционно сложные операции резервного копирования, репликации и восстановления, а также поддерживает большинство популярных приложений резервного копирования, уже развернутых в ЦОД.

Компания ESG начала проверочное тестирование с краткого обзора интерфейса управления InfiniGuard. На Рис. 8 показан 1 петабайт хранилища с двумя контроллерами дедупликации (DDE App A и DDE App B) по 400 ТБ на каждый плюс 200 ТБ, отведенные под моментальные снимки. Обратите внимание, как этот интуитивный пользовательский интерфейс позволяет отслеживать доступную емкость и дедупликацию для каждого тома. Если бы выполнялись какие-то задания резервного копирования, то вся активность отображалась бы напротив двух активных контроллеров дедупликации вверху слева, а коэффициент уменьшения объема данных был бы в среднем равен 10:1.

Рис. 8. Обзор интерфейса управления InfiniGuard



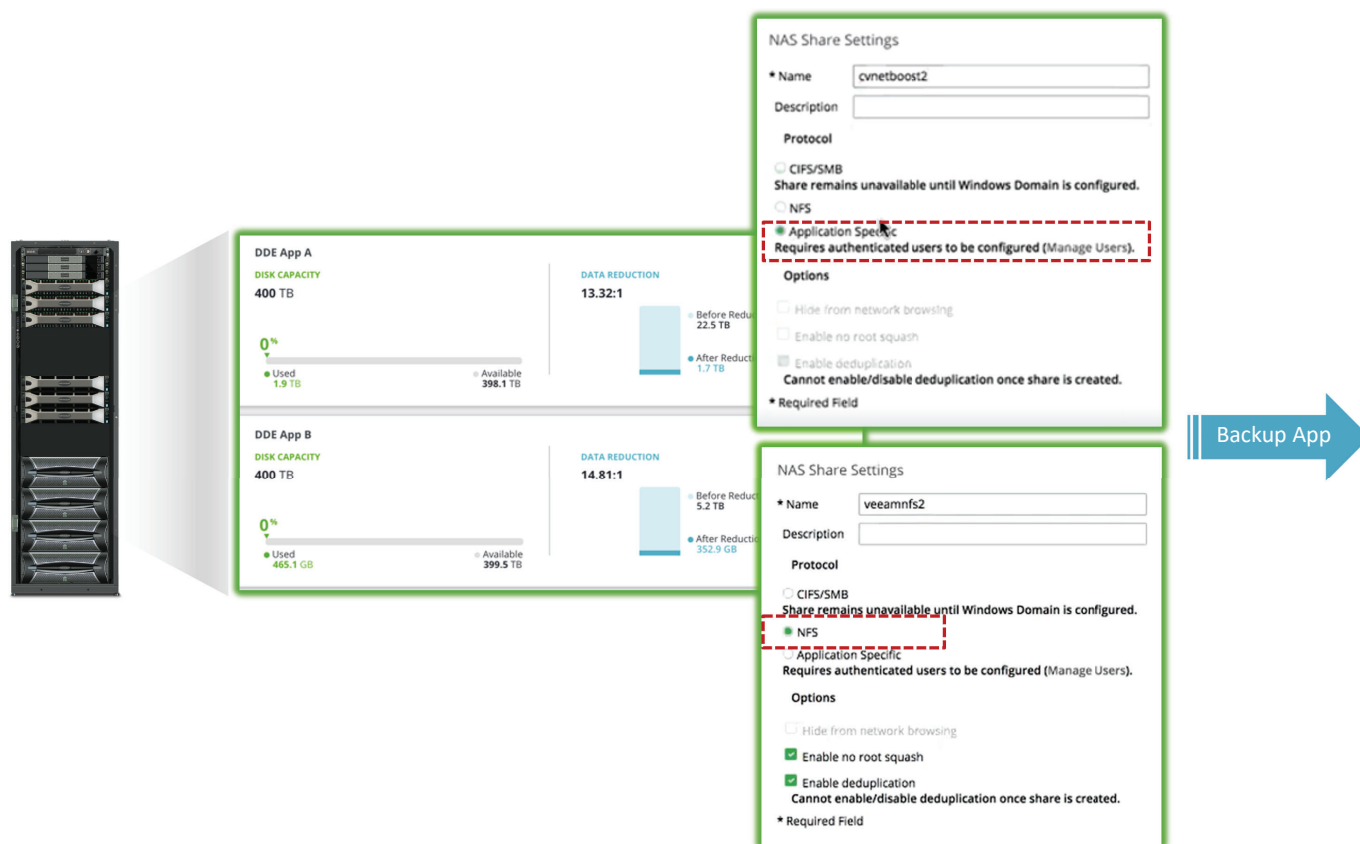
Источник: Enterprise Strategy Group

Состояние системы отображается вверху в центре интерфейса управления, где индикатор состояния сейчас показывает “peak health [полностью здоров]”. Для получения подробных сведений выберите “system health [состояние системы]” на левой боковой панели, чтобы открыть динамический пользовательский интерфейс, в котором вы можете нажать на предупреждение, как показано справа внизу на Рис. 8. В этом случае мы увидим отказавший диск, требующий внимания. Благодаря архитектуре с высокой степенью избыточности система может выдерживать многие типы сбоев, и они не будут влиять на производительность или емкость. Системные моментальные снимки также можно сделать неизменяемыми, что дает пользователям дополнительную защиту и возможность восстановления после кибератак. События записываются в журнал, и можно настраивать правила выдачи оповещений о событиях по протоколу SNMP или SMTP. Управление пользователями системы производится с помощью Active Directory по протоколу LDAP.

На вкладке конфигурации можно легко выделять общие дисковые сетевые ресурсы InfiniGuard для приложений защиты данных. На Рис. 9 показано выделение двух новых общих дисковых сетевых ресурсов NAS. Чтобы создать общий дисковый сетевой ресурс NAS, сначала мы присвоили ему имя и выбрали протокол. Варианты протоколов: CISF, SMB, NFS и Application Specific [Определяется приложением]. В этом примере для включения дедупликации на стороне источника был выбран протокол NetBoost, определяемый конкретным приложением.

На Рис. 9 показано, как на паре контроллеров дедупликации данных были созданы два общих дисковых сетевых ресурса. Опция “configure” использовалась для настройки параметров репликации (тип репликации, IP-адрес удаленного устройства InfiniGuard и учетные данные для доступа).

Рис. 9. Выделение общих дисковых сетевых ресурсов InfiniGuard для приложений защиты данных

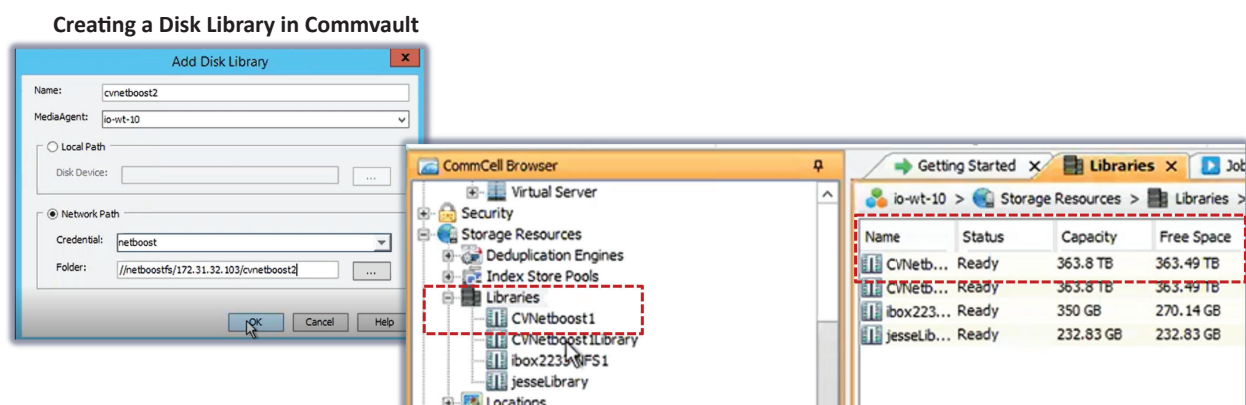


Источник: Enterprise Strategy Group

InfiniGuard работает с большинством основных решений для резервного копирования и восстановления, повышая их производительность и обеспечивая передовые технологии дедупликации и сжатия. Настроить InfiniGuard для работы с вендором резервного копирования, выбранным заказчиком, совсем не сложно. На Рис. 10 показано конфигурирование системы для работы с Commvault путем настройки общих ресурсов SMB, NFS или NetBoost. В данном примере был настроен протокол NetBoost. Процесс начинается в InfiniGuard с открытия вкладки Deduplication Engine [Контроллер дедупликации] на левой боковой панели. Затем мы добавили имя общего ресурса (cvnetboost2) и выбрали параметр “application specific [определяется приложением]”, чтобы включить протокол NetBoost. Наконец, мы присвоили IP-адрес этому новому общему дисковому сетевому ресурсу и настроили учетные данные Commvault.

Чтобы запустить первоначальное полное резервное копирование, мы использовали интерфейс управления Commvault для создания нового задания (или редактирования уже существующего), а в качестве имени нового тома резервного копирования указали точку монтирования InfiniGuard (см. Рис. 10). Мы запустили задание по запросу, и первое полное резервное копирование началось. Отсюда же мы запланировали инкрементальное резервное копирование. Как видно, создание и настройка InfiniGuard для работы с Commvault или другим ПО резервного копирования – это легко и просто.

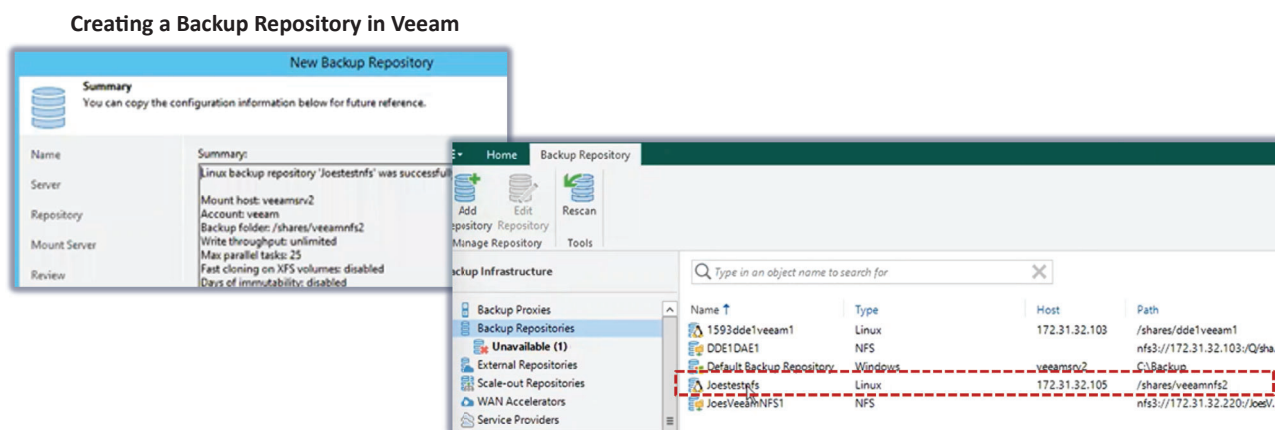
Рис. 10. Настройка Commvault для использования общего дискового сетевого ресурса InfiniGuard по протоколу NetBoost



Источник: Enterprise Strategy Group

InfiniGuard глубоко интегрируется с ПО резервного копирования и репликации Veeam. Чтобы создать репозиторий резервных копий InfiniGuard в Veeam, мы просто выбрали смонтированное хранилище с файловой системой NFS, которое было ранее создано с помощью интерфейса управления InfiniGuard (то есть созданное ранее хранилище DDE1DAE1, как показано на Рис. 11).

Рис. 11. Общий NFS-ресурс InfiniGuard для Veeam



Источник: Enterprise Strategy Group



Почему это важно

Согласно исследованию ESG, 75% респондентов считают, что за последние два года сложность ИТ-систем возросла. Кроме того, наиболее частой целью цифровой трансформации остается повышение эксплуатационной эффективности (56%).⁴

Компания ESG подтвердила, что InfiniGuard отличается легкостью развертывания, управления и интеграции с ведущим ПО резервного копирования. ESG также отметила легкость защиты данных резервного копирования с помощью неизменяемых моментальных снимков. В целом решение InfiniGuard упростило мониторинг, управление и составление отчетов по инфраструктуре, а также повысило эксплуатационную эффективность.

⁴ Источник: Исследовательский отчет ESG, [Обзор планируемых расходов на технологии в 2021 г.](#), январь 2021 г.

Резюме

Сейчас все чаще организации пересматривают свои стратегии защиты данных. Они анализируют старые практики, чтобы найти экономически эффективный способ повысить скорость и надежность своей инфраструктуры резервного копирования и аварийного восстановления.

Устаревшая архитектура некогда лучших в отрасли специализированных устройств резервного копирования с трудом пытается экономически эффективно удовлетворить потребности в защите данных рабочих нагрузок ключевых бизнес-приложений в петабайтном масштабе. Унаследованные решения были разработаны более 20 лет назад для сокращения окон резервного копирования и снижения стоимости защиты данных в дисковых системах хранения. С тех пор в большинстве организаций осознали, что, хотя производительность резервного копирования важна, время восстановления еще важнее – особенно после кибератаки. Поэтому многие организации пытаются обосновать необходимость затрат на обновление парка разнородных устаревших (и продолжающих устаревать) специализированных устройств резервного копирования до all-flash устройств последнего поколения.

Система InfiniGuard построена на базе специализированной архитектуры системы основного хранения данных InfiniBox, чтобы экономически эффективно удовлетворять потребности в хранении резервных копий организаций, оказывающих услуги резервного копирования и восстановления в петабайтном масштабе. В системе InfiniGuard используются диски вместо флеш-памяти для получения большой емкости, DRAM-кэш (который в 1000 раз быстрее диска) для ускорения обработки оперативных и “горячих” данных, а также SSD-кэш для “теплых” данных. InfiniGuard построен на проверенной опытом архитектуре InfiniBox с добавлением новейших технологий дедупликации и сжатия (включая опциональную дедупликацию на стороне источника), функциональной совместимости с решениями для резервного копирования и базами данных от ведущих игроков рынка, а также модели ценообразования, при которой всегда доступен полный функционал, а оплата производится по количеству потребляемой емкости. Благодаря этой уникальной архитектуре система InfiniGuard обеспечит чрезвычайно быстрое восстановление без ущерба для окон резервного копирования и для бюджета.

Компания ESG подтвердила легкость развертывания и управления InfiniGuard с помощью лучших в отрасли программ резервного копирования и баз данных. Мгновенное восстановление из неизменяемого моментального снимка InfiniGuard с помощью ПО резервного копирования Veeam обеспечило быстрое и безопасное восстановление после имитации атаки программы-вымогателя. Тестирование производительности с БД Oracle объемом 2 ТБ подтвердило, что InfiniGuard превосходит ожидания и обеспечивает скорости резервного копирования и восстановления, отвечающие требованиям к решениям корпоративного класса. Заказчик, с которым беседовала компания ESG, сообщил, что после замены его старой системы на InfiniGuard скорость резервного копирования и восстановления увеличилась на 284%, а емкость хранилища резервных копий уменьшилась на 97% (коэффициент сокращения примерно 32:1).

Если ваша организация пытается обосновать необходимость затрат на обновление устаревшего специализированного устройства защиты данных для выполнения соглашений об уровне обслуживания в части требований к восстановлению данных и устойчивости к кибератакам в петабайтном масштабе, то InfiniGuard – это хороший выбор.

Приложение

Таблица 1. Проверочный тестовый стенд

Целевое хранилище для резервных копий	
InfiniGuard, версия 3.5	(1) Контроллер дедупликации А с хранилищем емкостью 1 ПБ и портами 10GbE (2) Контроллер дедупликации В с хранилищем емкостью 1 ПБ и портами 10GbE
Приложение резервного копирования	
Veritas NetBackup, версия 8.2	(1) Media Server под CentOS 7 с двумя сетевыми картами 10GbE (2) Media Server под CentOS 7 с двумя сетевыми картами 10GbE (3) Media Server под CentOS 7 с двумя сетевыми картами 10GbE (4) Media Server под CentOS 7 с двумя сетевыми картами 10GbE (5) Media Server под CentOS 7 с двумя сетевыми картами 10GbE (6) Media Server под CentOS 7 с двумя сетевыми картами 10GbE (7) Media Server под CentOS 7 с двумя сетевыми картами 10GbE (8) Media Server под CentOS 7 с двумя сетевыми картами 10GbE
Сеть резервного копирования	
Nexus	(1) Model 3500, скорость 10GbE (2) Model 3500, скорость 10GbE

Все торговые наименования являются собственностью их соответствующих владельцев. Информация, содержащаяся в этой публикации, была получена из источников, которые компания Enterprise Strategy Group (ESG) считает надежными, но компания ESG не дает гарантий в отношении этой информации. Эта публикация может содержать мнения компании ESG, которые могут время от времени изменяться. Авторские права на эту публикацию принадлежат компании The Enterprise Strategy Group, Inc. Любое воспроизведение или дальнейшая передача данной публикации (полностью или частично, в печатном, электронном или ином виде) лицам, не имеющим прав на ее получение, без прямого согласия Enterprise Strategy Group, Inc. нарушает закон США об авторском праве, и против виновных будет возбужден иск о возмещении гражданского ущерба и, если применимо, уголовное преследование. С любыми вопросами вы можете обратиться в отдел по работе с клиентами компании ESG по телефону 508.482.0188.



Компания **Enterprise Strategy Group** занимается ИТ-аналитикой, исследованиями, проверкой и разработкой стратегий и предоставляет глобальному ИТ-сообществу рыночную информацию и практические советы.

The Enterprise Strategy Group, Inc., © 2021. Все права защищены.

