BlackArmor® NAS 220

Руководство пользователя BlackArmor® NAS 220

Seagate Technology LLC
920 Disc Drive
Scotts Valley CA 95066 U.S.A. (США)

Информация об открытом и лицензированном исходном коде

Информацию об открытом исходном коде и лицензиях, использованных в продуктах Seagate, можно получить на веб-сайте Seagate по адресу www.seagate.com/support.

Оглавление

1. Введение

- Об этом руководстве
- Содержимое комплекта поставки
- Системные требования
- Поиск дополнительной информации

Об этом руководстве

В этом *руководстве пользователя* предоставлены все сведения, необходимые для надлежащей настройки и использования сервера Seagate BlackArmor® NAS 220 (сервера BlackArmor).

В этом руководстве содержатся полные инструкции по установке, а также справочные сведения по компонентам функциям сервера BlackArmor. Содержит также обзор полноценного использования сервера BlackArmor при увеличении потребностей и появлении изменений в структуре и объеме данных.

Примечание. Пошаговые инструкции по использованию программных инструментов BlackArmor содержатся в интерактивной справочной системе, которая поставляется вместе с программным обеспечением.

Некоторые из разделов в этом руководстве предназначены только для *администраторов* BlackArmor, то есть для пользователей, которые имеют доступ к административным функциям сервера BlackArmor. Четко указывается информация, предназначенная только для администраторов.

Содержимое комплекта поставки

В содержимое комплекта поставки сервера BlackArmor входят следующие компоненты:

- сервер BlackArmor;
- адаптер питания;
- Ethernet-кабель;
- установочный компакт-диск, на котором содержится программное обеспечение, документация по продукту и гарантийная информация;
- *краткое руководство по BlackArmor.*

Системные требования

Любой компьютер, используемый для доступа к серверу BlackArmor, должен соответствовать следующим требованиям.

- Компьютер Microsoft Windows® или Apple Macintosh®, работающий под управлением одной из следующих операционных систем.
  - Windows XP, Windows Vista® или Windows 7 с самыми последними установленными пакетами обновления.
  - Mac OS X 10.4.11 или более поздняя версия.
- Сетевая карта.
- Поддерживаемые веб-браузеры:
  - Microsoft Internet Explorer 6, 7 или 8 (только Windows);
  - Apple Safari 3, 4 или более новая версия (Windows или Mac);
  - Mozilla Firefox 2, 3 или более новая версия (Windows или Mac).

Кроме того, понадобятся следующие компоненты.

- Локальная сеть (LAN) или беспроводная сеть (WLAN).
- Сетевой коммутатор или маршрутизатор хотя бы с одним доступным портом Ethernet 10/100/1000.
- Подключение к Интернету (для удаленного доступа к серверу и программному обеспечению, а также для обновления микропрограммного обеспечения).

Поиск дополнительной информации

Дополнительную информацию о сервере BlackArmor можно получить в следующих документах.

- Краткое руководство пользователя BlackArmor (напечатанный экземпляр).
- Справочная система по BlackArmor Manager.
- Справочная система по BlackArmor.
- Руководство пользователя BlackArmor Backup.
- Справочная система по BlackArmor Backup.

Дополнительную информацию можно получить на веб-сайте Seagate по адресу www.seagate.com.

2. Все о Seagate BlackArmor® NAS 220

- Введение
- О сервере BlackArmor
- Что можно делать с помощью сервера BlackArmor
- Различие между администратором и пользователем BlackArmor
- Как приступить к работе

Введение

В этой главе представлены компоненты и функции сервера BlackArmor® NAS 220 (сервер BlackArmor), описано назначение сервера BlackArmor и обозначены различия между администраторами BlackArmor и обыкновенными пользователями BlackArmor.

В этой главе также содержатся рекомендации по настройке и использованию сервера BlackArmor. (Чтобы узнать, являетесь ли вы администратором или пользователем, см. раздел «Различие между администратором и пользователем BlackArmor» на стр. 13.)

О сервере BlackArmor

Сервер BlackArmor является файловым сервером – устройством, которое используется для хранения всех типов компьютерных файлов и получения к ним доступа по локальной сети. Сервер BlackArmor содержит два дисковых накопителя Serial ATA (SATA) и имеет встроенную защиту данных от сбоев и других аварийных случаев.

Сервер BlackArmor поставляется в комплекте с программным обеспечением, которое можно использовать для резервного копирования, сохранения и защиты файлов, а также для предоставления к ним общего доступа.

Как правило, сервер BlackArmor поддерживает до 20 пользователей и используется владельцами предприятий малого бизнеса и пользователями, работающими в домашних офисах, которые хотят сохранять и защищать важные компьютерные файлы: клиентские файлы, бизнес-записи, финансовую информацию и т. д., а также предоставлять другим людям в своей локальной сети доступ к этим файлам.

Основные компоненты комплекта поставки сервера BlackArmor

Комплект поставки сервера BlackArmor состоит из четырех основных компонентов:

- **Сервер BlackArmor** – оборудование, оснащенное дисковыми накопителями для хранения и защиты файлов.
- **BlackArmor Discovery** – программное обеспечение, которое служит для обнаружения и подключения сервера BlackArmor к компьютеру.
- **BlackArmor Manager** – встроенный в сервер инструмент, который используется для настройки, изменения параметров и отслеживания сервера BlackArmor с компьютера пользователя через веб-браузер.
- **BlackArmor Backup** – программное обеспечение, с помощью которого можно создавать резервные копии файлов, приложений и даже операционных систем на сервере BlackArmor. С помощью этой программы также можно восстанавливать систему и данные. Дополнительные сведения см. в *руководстве пользователя BlackArmor*.

Функции сервера BlackArmor

Примечание. Функции, описанные в этом разделе, представлены в графическом виде на стр. 11.

Сервер BlackArmor состоит из следующих физических компонентов:

- Два дисковых накопителя Serial ATA (SATA) с возможностью замены пользователем.
- Один порт Ethernet или *порт локальной сети*, с помощью которого можно получать доступ к серверу из локальной сети или из Интернета.
- Два порта USB, которые используется для прямого резервного копирования данных с помощью портативного USB-накопителя или для подключения USB-принтера, которым смогут пользоваться все пользователи в локальной сети. Кроме того, к этим портам можно подключить ИБП.
- Светодиодные индикаторы, представляющие порт Ethernet, дисковые накопители и сервер, указывают на активность состояние компонентов. См. стр. 44.
- Кнопка сброса, позволяющая сбрасывать имя сервера BlackArmor, настройку DHCP (режим сети), а также имя пользователя и пароль для входа.

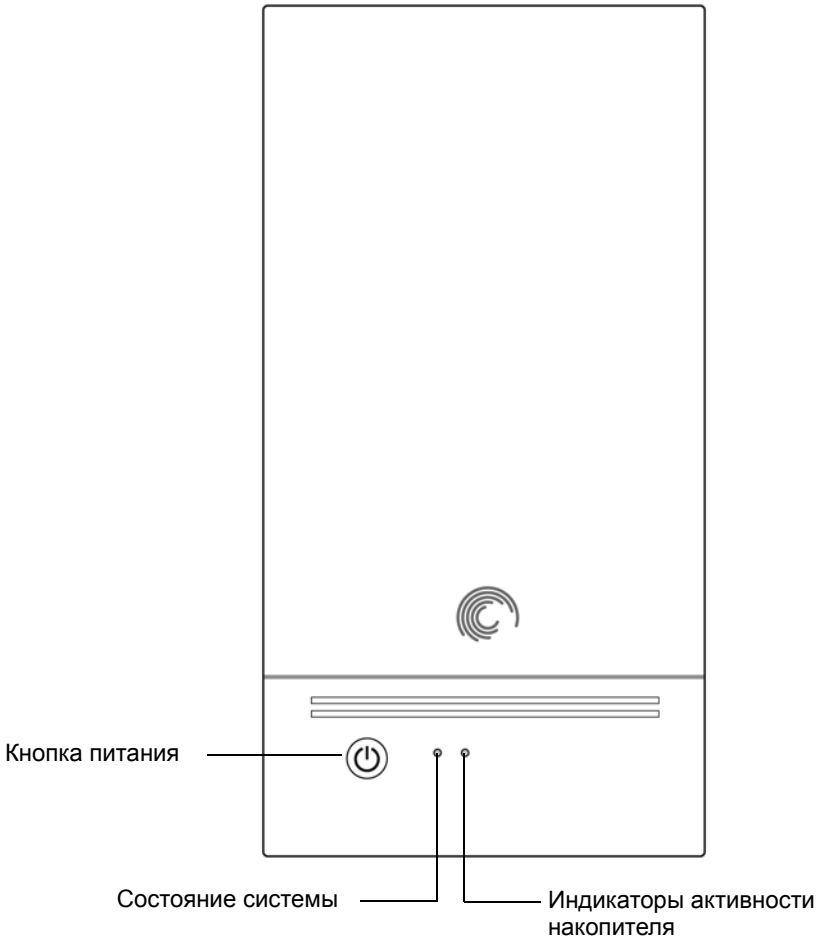


Рисунок 3. Передняя панель сервера BlackArmor

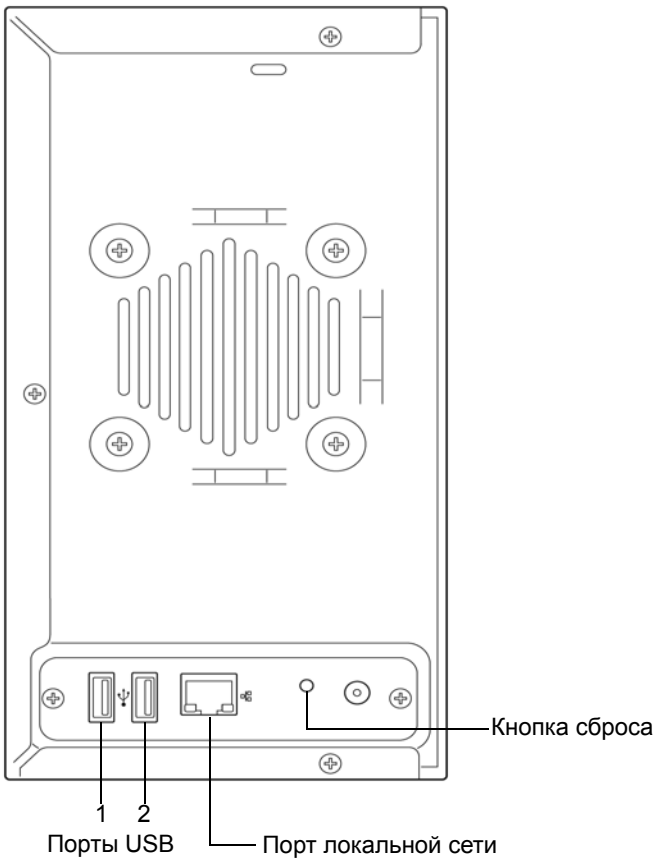


Рисунок 4. Задняя панель сервера BlackArmor

Что можно делать с помощью сервера BlackArmor

Сервер BlackArmor можно использовать в следующих целях:

- Создавать централизованное место хранения файлов, к которым необходимо предоставить доступ другим людям локальной сети или в Интернете.
- Создавать и поддерживать автоматические резервные копии всех файлов, а также операционных систем.
- Предоставлять общий доступ к файлам (контрактам, бизнес-презентациям, отчетам о выполнении работы и т. п.) другим пользователям в локальной сети или бизнес-клиентам в Интернете.
- Быстро восстановите компьютер после сбоя, такого как непреднамеренное удаление важных файлов или сбой дискового накопителя, а также после утери или кражи компьютера.

- Получать доступ к серверу BlackArmor по Интернету практически отовсюду и загружать необходимые файлы с сервера, а также выкладывать, находясь в поездке, файлы на сервер в целях их защиты и предоставления к ним общего доступа.
- Предоставлять доступ к USB-принтеру другим пользователям в локальной сети.
- Создавать мультимедийный сервер, чтобы все пользователи в локальной сети могли без труда загружать фотографии, видео и музыку.
- Включать на сервере службу iTunes®, чтобы пользователи могли слушать потоковую музыку на своем компьютере с установленным приложением iTunes.

Различие между администратором и пользователем BlackArmor

Помимо таких функций, как общий доступ к файлам, которыми могут пользоваться все пользователи, на сервере BlackArmor имеются административные функции, работающие в фоновом режиме, к которым имеют доступ один или два пользователя. Такие пользователи называются в этом руководстве *администраторами* BlackArmor.

Любой человек, имеющий доступ к серверу BlackArmor, называется в этом руководстве *пользователем* BlackArmor.

Сведения об администраторах BlackArmor

Администраторы BlackArmor имеют полный доступ ко всем функциям и параметрам сервера BlackArmor, а также ко всем хранящимся на них файлам. Администратор BlackArmor может выполнять следующие действия:

- изменять любой параметр сервера;
- создавать и изменять учетные записи пользователей и групп;
- создавать и изменять папки (или *общедоступные ресурсы*);
- обновлять микропрограммное обеспечение сервера;
- заменять поврежденный накопитель;
- сбрасывать имя и пароль для входа на сервер до исходных значений.

Информация о пользователях BlackArmor

Все пользователи BlackArmor, включая администраторов, могут выполнять следующие действия:

- изменять собственный пароль для входа;
- сохранять файлы на сервере BlackArmor и предоставлять к ним общий доступ;
- создавать резервные копии файлов на сервере BlackArmor с помощью BlackArmor Backup;
- получать доступ к серверу BlackArmor через Интернет с помощью службы Seagate Global Access;
- загружать большие файлы из Интернета напрямую на сервер BlackArmor;
- получать доступ к музыке, видео и фотографиям (если сервер BlackArmor является мультимедийным сервером);
- предоставлять доступ к USB-принтеру, подключенному к серверу BlackArmor (при наличии такого принтера).

Примечание. Администратор также может создавать учетные записи пользователей с административными привилегиями. Инструкции можно получить в интерактивной справочной системе по BlackArmor Manager.

Как приступить к работе

В этом разделе описываются задачи, которые следует выполнить администраторам и пользователям BlackArmor, приступая к работе с сервером.

Администраторы BlackArmor могут начать здесь

Чтобы начать работу с сервером BlackArmor, выполните следующие действия.

1. Установите сервер BlackArmor и соответствующее программное обеспечение (см. стр. 18).
2. Подключитесь к серверу с помощью инструмента BlackArmor Discovery (см. стр. 19).
3. Выполните исходную настройку сервера с помощью BlackArmor Manager (см. стр. 20).
4. Создайте общедоступные ресурсы для хранения файлов (см. стр. 21).
5. Создайте учетные записи для всех пользователей, которые будут работать с сервером BlackArmor, и назначьте каждому пользователю права на доступ к этим созданным общедоступным папкам (см. стр. 22).
6. Предоставьте каждому пользователю BlackArmor информацию о его учетной записи (см. стр. 23).

7. *(Дополнительно.)* Предоставление доступа к серверу BlackArmor через Интернет путем включения службы Global Access в приложении BlackArmor Manager (см. стр. 23).
8. *(Дополнительно.)* Сделайте USB-принтер доступным всем пользователям в локальной сети, подключив его к серверу BlackArmor (см. стр. 25).
9. *(Дополнительно.)* Подключите источник бесперебойного питания к серверу BlackArmor для наличия питания даже в случае отключения электроэнергии (см. стр. 48).
10. *(Дополнительно.)* Преобразование сервера BlackArmor в мультимедийный сервер, чтобы пользователи BlackArmor могли получать доступ к музыке, фотографиям и видео (см. стр. 26).
11. Продолжите выполнение инструкций «Пользователи BlackArmor могут начать здесь» на стр. 15 в следующем разделе, где описывается, как использовать сервер BlackArmor для сохранения, защиты и предоставления общего доступа к файлам.

Пользователи BlackArmor могут начать здесь

Чтобы начать работу с сервером BlackArmor, выполните следующие действия.

1. Убедитесь, что администратор BlackArmor предоставил вам следующее:

- программное обеспечение BlackArmor Discovery;
- программное обеспечение BlackArmor Backup;
- имя и пароль для входа в BlackArmor;
- имена общедоступных папок, к которым у вас будет доступ;
- описание любых ограничений доступа (например, доступ только на чтение к определенной общедоступной папке);
- копия руководства пользователя BlackArmor NAS 220

2. Установите программное обеспечение BlackArmor (см. стр. 18).

Примечание. Нет необходимости устанавливать BlackArmor Backup, если уже используется другое программное обеспечение для регулярного создания резервных копий.

3. Подключитесь к серверу и общедоступным папкам, к которым имеется доступ, используя BlackArmor Discovery (см. стр. 19).

4. Предоставьте общий доступ к файлам путем сохранения их на общедоступных ресурсах, к которым будут получат доступ другие пользователи в локальной сети или из Интернета.
5. *(Дополнительно.)* Создайте полную резервную копию важных файлов или настройте регулярное резервное копирование с помощью приложения BlackArmor Backup (см. стр. 57).
6. *(Дополнительно.)* Если к серверу BlackArmor был подключен USB-сервер, добавьте его в список доступных принтеров, следуя инструкциям используемой операционной системы.

3. Начало работы с сервером BlackArmor®

- Введение
- Действия по настройке для администраторов
- Начало работы в качестве пользователя BlackArmor

Введение

В этом разделе содержатся пошаговые инструкции по установке и настройке сервера BlackArmor® и соответствующего программного обеспечения.

Если вы не являетесь администратором BlackArmor, перейдите на стр. 28.

Примечание. Обзор действий по установке см. в разделе «Как приступить к работе» на стр. 14.

На этой схеме показано расположение сервера BlackArmor и место установки программного обеспечения.

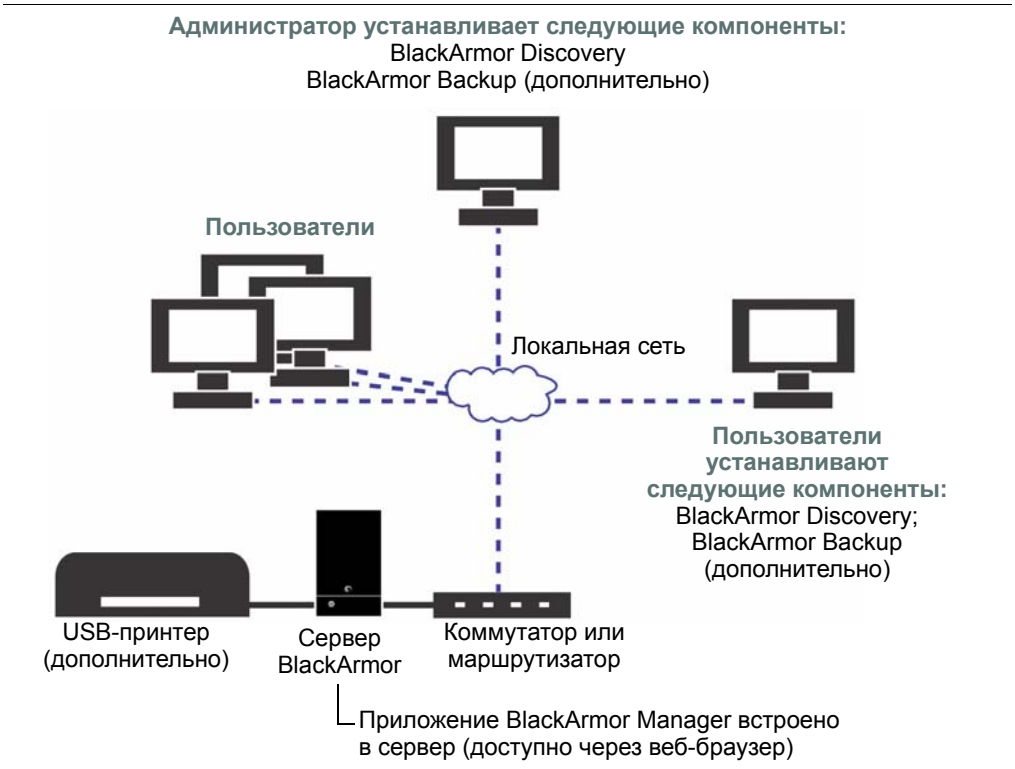


Рисунок 3. Стандартная установка и настройка BlackArmor

Действия по настройке для администраторов

Если вы не являетесь администратором BlackArmor, перейдите на стр. 28.

Установка сервера BlackArmor и программного обеспечения

Прежде чем приступить к работе:

- убедитесь, что используемый компьютер соответствует системным требованиям, приведенным на стр. 8;
- убедитесь, что сервер установлен на прочной, ровной поверхности в помещении с надежной вентиляцией; убедитесь, что вентиляционные отверстия на сервере не закрыты или заблокированы и что сервер не размещен рядом с источником тепла; убедитесь, что сервер не расположен в тех местах, где на него могут быть пролиты какие-либо жидкости.

Чтобы установить сервер и программное обеспечение BlackArmor, выполните перечисленные ниже действия.

1. Используйте кабель Ethernet, входящий в комплект поставки, для подключения сервера BlackArmor к коммутатору или маршрутизатору в локальной сети. Подключите кабель Ethernet к порту локальной сети, как показано ниже.

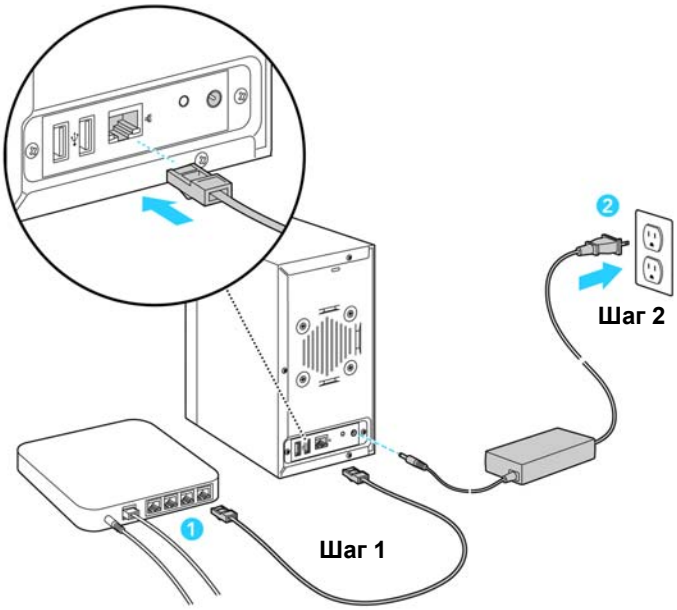


Рисунок 4. Подсоедините кабель питания и сетевые кабели

2. Используйте входящий в комплект адаптер питания для подключения сервера BlackArmor к заземленной розетке электропитания.

Сервер включится автоматически, и загорятся индикаторы на передней панели сервера.

3. Вставьте в компьютер установочный компакт-диск.

Мастер установок открывается автоматически. Установите приложения BlackArmor Discovery *и* BlackArmor Backup, если только вы не используете другое программное обеспечение для резервного копирования.

4. Нажмите на кнопку **Далее**.
5. Нажмите кнопку **Далее**, чтобы разрешить установку в папку по умолчанию, или кнопку **Обзор**, чтобы выбрать другое место установки, затем нажмите кнопку **Далее**.
6. Нажмите кнопку **Далее** для установки программы в папку по умолчанию или введите пользовательское имя и нажмите кнопку **Далее**.

Будет установлено приложение BlackArmor Discovery.

Нажмите кнопку **Готово**.

Подключение к серверу

Чтобы подключиться к серверу BlackArmor, выполните следующие действия.

1. Дважды щелкните значок BlackArmor Discovery на рабочем столе (Windows) или в папке «Программы» (Mac).

При открытии BlackArmor запускается автоматический поиск всех серверов BlackArmor в локальной сети с последующим отображением списка результатов.

2. Выберите новый сервер BlackArmor.
3. (Windows) Щелкните **Просмотр информации о накопителе**, затем щелкните пункт **Управление**. (Mac) Щелкните пункт **Управление сервером**.

Будет открыто приложение BlackArmor.

Примечание. Приложение BlackArmor Discovery останется открытым, если не будет закрыто вручную. Если вы закрыли приложение, то можете открыть его любое время двойным щелчком по значку на рабочем столе (Windows) или в папке «Приложения» (Mac).

4. Войдите в систему, используя настройки по умолчанию. (Имя пользователя и пароль вводятся с учетом регистра.)

Имя пользователя: **admin**

Пароль: **admin**

Примечание. Другие настройки сервера BlackArmor также заданы по умолчанию, что поможет вам сразу начать сохранение, совместное использование и защиту файлов. Дополнительные сведения см. в разделе стр. 33.

Завершение начальной настройки

Когда вы в первый раз входите на сервер BlackArmor, открывается окно мастера настройки. Чтобы завершить настройку, выполните следующие действия.

1. Нажмите кнопку **Далее**, чтобы начать исходную настройку сервера BlackArmor.
2. Прочтите лицензионное соглашение Seagate BlackArmor и щелкните пункт **Я согласен**.
3. Для настройки базовых параметров сервера выполните следующие действия.

- Введите имя сервера BlackArmor. Чтобы сделать сервер узнаваемым и упростить его определение в локальной сети, задайте для него уникальное и легко запоминающееся имя. Имя может содержать до 16 буквенно-цифровых символов и может включать дефисы. Использование пробелов недопустимо.
- Введите описание сервера, используя местоположение, содержимое и другие характеристики сервера, которые помогут вам отличить его от других серверов в локальной сети.

4. Выберите часовой пояс, соответствующий местоположению сервера, а затем установите текущую дату и время.
5. Нажмите на кнопку **Далее**.
6. Введите два раза новый пароль администратора, затем нажмите кнопку **Далее**.

Seagate настоятельно рекомендует настроить пароль администратора для защиты сервера BlackArmor и его содержимого. Пароли могут содержать до 16 букв и цифр и чувствительны к регистру.

Пример надежного пароля: **LEag29ue**

Пример ненадежного пароля: **blackarmor**

7. Выберите сетевой режим, а затем нажмите кнопку **Далее**.

По умолчанию сетевой режим сервера BlackArmor задан как DHCP.

Если вы не являетесь сотрудником большой корпорации, имеющей собственный отдел ИТ, компания Seagate настоятельно рекомендует использовать DHCP в своей сети.

8. Нажмите кнопку **Далее**, чтобы завершить настройку.
9. Просмотрите сводные данные настройки. Щелкните **Назад** для внесения каких-либо изменений или **Готово** для завершения настройки.

Создание пользовательских общедоступных ресурсов

Сервер BlackArmor имеет два предварительно настроенных общедоступных ресурса: «Загрузка» и «Общий». Если эти два общедоступных ресурса соответствуют вашим потребностям, перейдите к разделу «Создание учетных записей пользователей» на стр. 22.

Можно также создавать собственные пользовательские общедоступные ресурсы с помощью веб-интерфейса BlackArmor Manager. Это можно сделать для сохранения файлов по категории, например клиентских файлов, файлов проекта или финансовых архивных файлов, а также для сохранения файлов по бизнес-отделам, таким как маркетинг, бухгалтерия или отдел продаж.

Чтобы создать пользовательские общедоступные ресурсы, выполните следующие действия.

1. На панели меню выберите **Хранилище**, щелкните **Общедоступные ресурсы**, затем щелкните значок **Добавить**.
2. Введите имя нового общедоступного ресурса.

Чтобы сделать общедоступный ресурс более узнаваемым на сервере, дайте ему уникальное имя, которое было бы описательным и легко запоминаемым.

3. Введите описание для этого общедоступного ресурса.
4. Выберите владельца общедоступного ресурса из раскрывающегося списка всех учетных записей пользователей. (Информацию о создании отдельных учетных записей пользователей см. в разделе «Создание учетных записей пользователей» на стр. 22.)
5. Выберите типы протоколов, которые будут поддерживаться этим общедоступным ресурсом (см. стр. 38).
6. Выберите том, на котором вы будете создавать общедоступный ресурс, если на сервере несколько томов.
7. Вы можете защитить файлы в общедоступном ресурсе от случайного удаления посредством добавления корзины в общедоступный ресурс. Удаленные файлы могут быть при необходимости восстановлены из корзины.

Чтобы добавить корзину, нажмите кнопку **Включить** рядом с пунктом **Корзина**.

8. Можно определить для общедоступного ресурса возможность загрузки определенных типов файлов в папки по умолчанию, например, все музыкальные файлы должны загружаться в папку «Музыка».

Чтобы автоматически упорядочить загруженные файлы, нажмите кнопку **Включить** рядом с пунктом **Перетаскивание и сортировка**. Информацию об этой службе см. в разделе «Специальные функции общедоступных ресурсов» на стр. 38.

9. Сервер BlackArmor можно использовать для организации общего доступа пользователей локальной сети к цифровым фотографиям, видеозаписям и музыкальным файлам, а также для потоковой передачи музыки iTunes. Чтобы настроить эту службу, нажмите кнопку **Включить** рядом с пунктом **Мультимедийная служба**.
10. Установите флажок **Общий доступ**, чтобы перейти на страницу создания и настройки прав доступа пользователей и групп к этому новому общедоступному ресурсу. Дополнительную информацию можно найти в интерактивной справочной системе по BlackArmor Manager.
11. Нажмите кнопку **Отправить**.

Будет создан общедоступный ресурс.

Создание учетных записей пользователей

На сервере BlackArmor содержится только одна учетная запись администратора. Следующим шагом является использование BlackArmor Manager для создания отдельных учетных записей пользователей.

Частью создания учетных записей пользователей является назначение каждому пользователю доступа к общедоступным ресурсам по умолчанию или к новым созданным вами общедоступным ресурсам.

Чтобы создать учетную запись пользователя, выполните следующие действия.

1. На панели меню выберите пункт **Доступ**, затем щелкните пункт **Пользователи**.
2. Щелкните значок **Добавить**.
3. Настройте учетную запись по своему желанию.

- **Имя пользователя**: имя пользователя, вводимое при входе.
- **Права администратора**: служит для определения пользователя в качестве администратора BlackArmor.
- **Полное имя**: имя пользователя.
- **Пароль** и **Подтверждение пароля**: до 16 буквенно-цифровых символов, которые пользователь вводит при входе.
- **Группа**: группа пользователей, к которой принадлежит данная учетная запись (при ее наличии).
- **Создание личного общедоступного ресурса пользователя**: должен или нет BlackArmor Manager создать новый личный общедоступный ресурс для этой учетной записи.

- **Том**: на каком томе (если их несколько) будет создан личный общедоступный ресурс.
- **Службы**: какие типы файловой службы должны поддерживаться личным общедоступным ресурсом.

4. Нажмите кнопку **Отправить**.

Новая учетная запись появляется в списке учетных записей пользователя.

Примечание. Можно упростить управление доступом к общедоступным ресурсам путем сортировки пользователей по группам. Управляя группами пользователей, изменяйте в одном окне доступ к общедоступным ресурсам как для отдельных пользователей, так и для целых групп. Дополнительные сведения см. в разделе стр. 41.

Распространение пользовательской информации BlackArmor

После создания учетных записей пользователей, предоставьте каждому пользователю BlackArmor следующие элементы, чтобы пользователи могли начать использовать сервер BlackArmor.

- Программное обеспечение BlackArmor Discovery;
- Программное обеспечение BlackArmor Backup (дополнительно).
- Имя и пароль пользователя BlackArmor
- Имена общедоступных ресурсов, к которым у этого пользователя будет доступ, а также все применимые ограничения доступа, например доступ только на чтение.
- Копия этого руководства и раздел, который должны прочитать пользователи, прежде чем начать использовать сервер BlackArmor («Пользователи BlackArmor могут начать здесь» на стр. 15).

Можно создавать копии программного обеспечения для каждого пользователя BlackArmor, используя прилагаемый компакт-диск или программное обеспечение, загруженное с сайта www.seagate.com/support.

Предоставление доступа к BlackArmor с помощью службы Seagate Global Access

Примечание. Этот шаг не является обязательным. Только администраторы BlackArmor могут включать глобальный доступ на сервере.

Можно сделать файлы и папки на сервере BlackArmor доступными в Интернете, включив службу Global Access в приложении BlackArmor Manager.

Seagate Global Access – это служба, позволяющая просматривать, загружать, предоставлять общий доступ и работать с файлами, которые хранятся на сервере BlackArmor из любой точки мира. Кроме того, вы можете использовать службу Global Access для загрузки файлов на сервер BlackArmor.

Чтобы получить доступ к серверу BlackArmor через Интернет, выполните следующие действия.

- Администратор должен включить службу Global Access на сервере с помощью приложения BlackArmor Manager. Это позволит получать удаленный доступ к серверу.
- Каждый пользователь, включая администратора, должен иметь учетную запись службы Global Access для использования этой функции. Любой пользователь, желающий получить доступ к серверу BlackArmor через Интернет должен иметь собственную учетную запись Global Access. (Учетные записи предоставляются бесплатно.)

Включение службы Global Access на сервере (задача выполняется администратором)

1. На панели меню выберите пункт **Доступ**, затем щелкните пункт **Global Access**.
2. Установите флажок **Включить**.
3. Нажмите кнопку **Отправить**.

Теперь доступ к серверу включен. Кроме того, пользователи должны создать учетную запись Seagate Global Access и включить службу Global Access, чтобы получить доступ к файлам на сервере через Интернет. См. «Создание учетной записи Seagate Global Access» на стр. 30.

Активация службы Global Access для пользователя

После того как администратор активировал на сервере службу Global Access, каждый пользователь должен активировать доступ для своей учетной записи.

Чтобы включить глобальный доступ, пользователь должен иметь учетную запись службы Seagate Global Access. Можно создать учетную запись на странице Global Access, описание которой приведено ниже. Подробные инструкции содержатся в разделе «Создание учетной записи Seagate Global Access» на стр. 30.

1. Войдите на сервер под своей учетной записью.
2. На панели меню выберите пункт **Global Access**. (Если учетная запись пользователя имеет права администратора, выберите пункт **Доступ**, затем щелкните **Global Access**.)
3. Установите флажок **Включить**.
4. Если вы не создавали учетную запись службы Global Access, щелкните **Создать учетную запись**. В противном случае переходите к шагу 5.

Появится новое окно веб-браузера. Следуйте инструкциям на экране для создания новой учетной записи.

5. Введите адрес электронной почты и пароль для учетной записи Seagate Global Access.
6. Нажмите кнопку **Отправить**.

В инструкциях пользователя по Global Access указано, как предоставлять доступ к файлам другим пользователям.

Войдите в свою учетную запись службы Seagate Global Access.

1. Войдите на сервер под своей учетной записью.
2. На панели меню выберите пункт **Global Access**.
3. Введите адрес электронной почты и пароль для доступа к своей учетной записи Seagate Global Access.
4. Щелкните пункт **Войти в учетную запись**.

В инструкциях пользователя по Global Access указано, как предоставлять доступ к файлам другим пользователям.

Подключение USB-принтера к серверу BlackArmor

Примечание. Этот шаг не является обязательным. Только администраторы BlackArmor могут настроить принтер.

Можно сделать USB-принтер доступным в локальной сети, подключив его к серверу.

Чтобы подключить принтер, выполните следующие действия.

1. Убедитесь, что принтер выключен.
2. Используйте высококачественный кабель USB для подсоединения принтера к одному из USB-портов на задней панели сервера BlackArmor.
3. Включите принтер и установите драйвер на компьютере (если это еще не сделано), следуя инструкциям производителя.
4. Попросите других пользователей в локальной сети добавить USB-принтер в списки доступных принтеров, следуя инструкциям в используемой операционной системе.

Принтер станет доступен всем пользователям BlackArmor. Диспетчер принтеров находится в меню «Сеть» приложения BlackArmor Manager. Дополнительная информация содержится в интерактивной справочной системе.

Настройка сервера BlackArmor в качестве мультимедийного сервера

Примечание. Этот шаг не является обязательным. Только администраторы BlackArmor могут включить функцию мультимедийного севера.

Сервер BlackArmor можно использовать для организации общего доступа пользователей локальной сети к цифровым фотографиям, видеозаписям и музыкальным файлам, а также для потоковой передачи музыки iTunes. Папки мультимедиа, в которые можно сохранять файлы («Наша музыка», «Наши изображения» и «Наше видео»), станут доступными после включения функции перетаскивания и сортировки в BlackArmor Manager. Дополнительную информацию можно найти в интерактивной справочной системе по BlackArmor Manager.

Чтобы настроить сервер BlackArmor в качестве мультимедийного сервера, выполните следующие действия.

1. На панели меню выберите **Мультимедиа**, а затем щелкните **Мультимедийная служба**.
2. Рядом с пунктом **Служба** выберите пункт **Включить**.
3. При необходимости установите метод сортировки по умолчанию для мультимедийных файлов, а затем щелкните **Отправить**.

Сервер BlackArmor может выполнять роль сервера iTunes, таким образом, пользователи BlackArmor могут слушать потоковую музыку прямо на компьютере с установленным приложением iTunes или на устройстве iPod, подключенном к компьютеру в сети.

4. Установите периодичность выполнения сервером поиска новой музыки. Вы можете установить время от каждых пяти минут до одного раза в день.
5. Нажмите кнопку **Отправить**, чтобы сохранить настройки.

Мультимедийная служба включена.

Создание папок для мультимедиа и музыки

Выполните приведенные ниже действия, если необходимо создать папки сервера мультимедиа.

1. Запустите приложение BlackArmor Discovery.
2. Выберите сервер.

- (Windows) Выберите сервер, затем щелкните пункт **Просмотр информации о накопителе**.
- (Mac) Выберите сервер в верхней таблице окна Discovery, затем щелкните пункт **Подключить общедоступный ресурс**, выбрав в нижней таблице общий общедоступный ресурс.

3. Выберите общий общедоступный ресурс и щелкните пункт **Просмотр** (Windows) или дважды щелкните подключенный общедоступный ресурс (Mac).

Будет открыт общедоступный ресурс.

4. Создайте следующие папки в точности как показано ниже. «Наша музыка», «Наши изображения», «Наше видео».

Теперь можно размещать свои файлы в соответствующих папках, расположенных на общедоступном ресурсе.

Дальнейшие шаги для администраторов

Прежде чем продолжить, следует ознакомиться с функциями сервера BlackArmor и соответствующего программного обеспечения, ознакомившись с этим руководством.

Сервер BlackArmor имеет предварительно заданные настройки, которые применимы для типичного использования, поэтому можно сразу начать сохранять и защищать файлы, а также предоставлять к ним общий доступ (см. стр. 33). В BlackArmor Manager можно настроить сервер BlackArmor в соответствии со своими потребностями.

После исходной настройки можно выполнить следующие действия.

- Настроить учетные записи групп для более простого управления разрешениями доступа (см. стр. 41).
- Настройте тома сервера и конфигурации RAID (см. стр. 36).
- Настроить непрерывный процесс резервного копирования, используя для этого второй сервер в сети (см. стр. 42).
- Хранить все фотографии, видео и музыкальные файлы на сервере и использовать последний в качестве мультимедийного сервера, чтобы находящиеся в сети проигрыватели мультимедиа могли получать доступ к файлам (см. стр. 43).
- Отслеживать сервер как локально, так и удаленно (см. стр. 43).

В оставшейся части этого руководства представлены функции сервера и некоторые рекомендации, которые помогут вам создать систему хранения, соответствующую вашим нуждам.

Примечание. Не забывайте, что вы также являетесь пользователем BlackArmor. Чтобы начать сохранение, резервное копирование и совместное использование файлов, перейдите к разделу «Начало работы в качестве пользователя BlackArmor» на стр. 28.

Начало работы в качестве пользователя BlackArmor

Выполните действия, приведенные в этом разделе, чтобы начать использовать сервер BlackArmor.

1. Убедитесь, что администратор BlackArmor предоставил вам следующее:
   - программное обеспечение BlackArmor Discovery;
   - имя и пароль для входа в BlackArmor;
   - Программное обеспечение BlackArmor Backup (дополнительно).
   - Имена общедоступных ресурсов, к которым у вас есть доступ
   - Описание любых ограничений доступа (например, доступ только на чтение к определенному общедоступному ресурсу)
   - Копия руководства пользователя BlackArmor NAS 220
2. Установите программное обеспечение BlackArmor.

   Установите приложения BlackArmor Discovery *и* BlackArmor Backup, если только вы не используете другое программное обеспечение для резервного копирования.
3. Подключитесь с помощью BlackArmor Discovery к серверу BlackArmor и расположенным на нем общедоступным ресурсам, к которым у вас есть право доступа.
   - (Windows) Дважды щелкните значок BlackArmor Discovery на рабочем столе.
   - (Mac) Дважды щелкните значок BlackArmor Discovery в папке «Программы».

   При открытии BlackArmor запускается автоматический поиск всех серверов BlackArmor в локальной сети с последующим отображением списка результатов.
4. Выберите новый сервер BlackArmor.

   Появится список всех общедоступных ресурсов, имеющихся на сервере (Mac). Щелкните пункт **Сервер управления**.
   - (Windows) Щелкните пункт **Просмотр информации о накопителе**. Появится список всех общедоступных ресурсов, имеющихся на сервере.
5. Используйте стрелки вверх и вниз для просмотра списка общедоступных ресурсов, затем выполните приведенные ниже действия.
   - Чтобы получить доступ к серверу с помощью BlackArmor Manager, щелкните пункт **Управление** и введите назначенное вам имя пользователя и пароль. Если у вас нет этих данных, свяжитесь с администратором.
   - Чтобы просмотреть общедоступные ресурсы, выберите общедоступный ресурс и щелкните пункт **Просмотр**.
   - Чтобы привязать общедоступный ресурс, выберите нужный ресурс и щелкните пункт **Привязать**.

- Если появится запрос, войдите в систему, используя свои имя пользователя и пароль BlackArmor. Общедоступный ресурс будет подключен. На рабочем столе появится соответствующий значок (Mac).
- (Windows) Выберите диск из раскрывающегося меню, затем нажмите **Да**. Общедоступному ресурсу будет назначена буква накопителя. Данный ресурс будет отображаться в проводнике Windows под соответствующей буквой.

- Если у вас есть доступ к нескольким общедоступным ресурсам, продолжите обнаружение и привязку дополнительных общедоступных ресурсов.

Примечание. Можно подключать или привязывать столько общих и личных общедоступных ресурсов, сколько потребуется. Однако, чтобы одновременно подключить несколько *личных* общедоступных ресурсов, для каждого личного общедоступного ресурса должны использоваться одни и те же учетные данные входа.

6. Сохраните файлы на общедоступных ресурсах, к которым будут получать доступ другие пользователи в локальной сети или из Интернета.

Дополнительные действия

- *(Дополнительно.)* Создайте полную резервную копию важных файлов или настройте регулярное резервное копирование с помощью приложения BlackArmor Backup (см. стр. 57).
- *(Дополнительно.)* Если к серверу BlackArmor был подключен USB-сервер, добавьте его в список доступных принтеров, следуя инструкциям используемой операцчтоыионной системы.
- *(Дополнительно.)* Если администратор BlackArmor включил службу мультимедиа на этом сервере и у вас есть доступ к общедоступному ресурсу, на котором сохранены музыкальные файлы, установите на своем компьютере приложение iTunes и начните слушать потоковую музыку, следуя инструкциям в приложении iTunes.
- *(Дополнительно.)* Если администратор BlackArmor включил на сервере службу Global Access, зарегистрируйтесь для получения бесплатной учетной записи Global Access, чтобы иметь возможность открывать файлы на сервере BlackArmor из сети Интернет. См. «Создание учетной записи Seagate Global Access» на стр. 30.

Создание учетной записи Seagate Global Access

Seagate Global Access – это служба, с помощью которой можно просматривать, загружать, предоставлять общий доступ и работать с файлами, хранящимися на сервере BlackArmor из любой точки мира, предоставлять общий доступ к файлам, хранящимся на личном общедоступном ресурсе, или совместно использовать ваши файлы с любым пользователем, находящимся за пределами локальной сети.

Чтобы создать учетную запись Seagate Global Access, выполните следующие действия.

1. Перейдите на веб-сайт Seagate Global Access, расположенный по адресу *http://globalaccess.seagate.com*.
2. Будет открыта страница входа на сайте Seagate Global Access. Щелкните ссылку для начала работы.
3. На странице входа в Seagate Global Access введите свой адрес электронной почты под надписью **Don't have an account?** (У вас нет учетной записи?) и нажмите **Send** (Отправить).
4. Страница будет обновлена, и появится сообщение об отправке вам электронного сообщения.

Служба Global Access отправляет приглашение на указанный вами адрес электронной почты; в присланном сообщении будет содержаться ссылка на веб-страницу, на которой можно будет открыть учетную запись Global Access. Выполните инструкции на экране для открытия учетной записи и входа в систему Global Access. Нажмите кнопку **Help** (Справка) на веб-сайте Global Access, чтобы ознакомиться с инструкциями по использованию Seagate Global Access.

4. Полноценное использование сервера BlackArmor®

- Введение
- Роль администратора BlackArmor
- Параметры севера BlackArmor по умолчанию
- УправлениеBlackArmor томами, общедоступными ресурсами и хранилищем
- Управление пользователями BlackArmor
- Защита файлов BlackArmor с помощью резервного копирования по сети
- Настройка сервера BlackArmor в качестве мультимедийного сервера
- Отслеживание состояния сервера BlackArmor
- Изменение расширенных настроек сервера BlackArmor
- Обслуживание сервера BlackArmor

Введение

В этой главе описываются функциональные возможности сервера BlackArmor® и соответствующего программного обеспечения, а также содержатся рекомендации для администраторов BlackArmor.

Некоторые функции сервера BlackArmor более подходят администраторам, которые считают себя опытными пользователями компьютеров. Разделы, посвященные этим функциям, обозначены соответствующим образом.

Примечание. Разделы в этой главе посвящены задачам, которые могут выполнять только администраторы BlackArmor. Если вы не являетесь администратором BlackArmor, перейдите к главе «Рекомендации для пользователей BlackArmor®» на стр. 53.

Роль администратора BlackArmor

Администраторы BlackArmor имеют полный доступ ко всем функциям и параметрам сервера BlackArmor, а также ко всем хранящимся на них файлам.

Роль администратора BlackArmor заключается в выполнении перечисленных ниже действий.

- Управление на сервере BlackArmor доступным свободным пространством для хранения путем создания и изменения томов и общедоступных ресурсов (см. стр. 34).
- Управление доступом к серверу путем создания учетных записей пользователей BlackArmor и управления ими (см. стр. 41).
- Обеспечивайте бесперебойную работу сервера BlackArmor путем отслеживания работоспособности сервера и его дисковых накопителей (см. стр. 43).
- Обеспечение бесперебойной работы сервера BlackArmor путем обновления микропрограммного обеспечения при появлении новых версий (см. стр. 50).

Вы как администратор BlackArmor можете воспользоваться перечисленными ниже преимуществами для эффективного использования сервера BlackArmor.

- Создавайте учетные записи групп для упрощения управления доступом к общедоступным ресурсам. Управляя группами пользователей, изменяйте в одном окне доступ к общедоступным ресурсам как для отдельных пользователей, так и для целых групп (см. стр. 41).
- Защищайте файлы, сохраненные на сервере BlackArmor, путем настройки регулярного создания резервных копий всего содержимого сервера (см. стр. 42).
- Настраивайте сервер BlackArmor в качестве мультимедийного сервера, чтобы пользователи BlackArmor могли слушать потоковую музыку прямо на своем компьютере или мультимедийном проигрывателе с установленным приложением iTunes (см. стр. 43).
- Экономьте электроэнергию путем *остановки* накопителей на сервере BlackArmor и перевода сервера в режим ожидания (см. стр. 47).
- Подключите сервер BlackArmor к источнику бесперебойного питания, что обеспечит достаточно электроэнергии для сохранения любых обрабатываемых файлов и правильного выключения питания сервера в случае перебоев с электроснабжением (см. стр. 48).
- *(Дополнительно.)* Убедитесь, что входящий трафик доходит до назначения, задав в BlackArmor Manager настройки динамической системы DNS (см. стр. 46).

В оставшейся части этой главы описываются параметры сервера BlackArmor по умолчанию, затем освещается использование прочих функций сервера, предназначенных для создания решения по хранению данных, соответствующего вашим потребностям.

Параметры севера BlackArmor по умолчанию

На сервере BlackArmor предварительно настроены параметры, которые подходят для типичного использования, поэтому можно сразу начать сохранение, обеспечение защиты и предоставление общего доступа к файлам.

- **Учетные записи пользователей** – сервер BlackArmor имеет одну предварительно настроенную учетную запись администратора, пароль которой можно изменить во время исходной настройки (см. стр. 20). В BlackArmor Manager можно также добавить другие учетные записи пользователей по мере необходимости (см. стр. 41).
- **Общедоступные ресурсы** – сервер BlackArmor содержит два предварительно настроенных общедоступных ресурса: «Загрузка» и «Общий». Можно изменять функции каждого общедоступного ресурса в соответствии со своими требованиями или добавлять новые общие или личные общедоступные ресурсы, используя для этого приложение BlackArmor Manager (см. стр. 37).
- **Защита RAID** – на сервере BlackArmor предварительно настроена защита RAID уровня 1. Эта технология позволяет использовать преимущества избыточности для системы хранения, чтобы защитить данные на накопителе от повреждений и прочих аварийных случаев. Защита RAID 1 заключается в «зеркалировании» данных сервера, то есть идентичные копии данных существуют на обоих дисках.

  Можно использовать массив RAID 0, также известный как «чередование», в котором данные равномерно распределяются (чередуются) между дисковыми накопителями равномерными блоками, а также составные тома, также известные как JBOD (просто группа накопителей). RAID 0 не обеспечивает защиту данных; составные тома не поддерживают защиту RAID.

  Дополнительные сведения см. в разделе стр. 36.
- **Параметры сети** – по умолчанию сервер работает в сетевом режиме DHCP. Рекомендуется использование DHCP. *DHCP* – это протокол динамической конфигурации узлов, который является методом автоматического назначения IP-адресов для всех систем в локальной сети. (При использовании статического режима все IP-адреса должны назначаться и изменяться вручную.)

  Если вы не являетесь сотрудником большой корпорации, имеющей собственный отдел ИТ, компания Seagate настоятельно рекомендует использовать DHCP в своей сети.
- **Пароль администратора** – по умолчанию для входа на сервер используются следующие данные.

  имя пользователя: admin

  пароль: admin

При исходной настройке сервера появится запрос на изменение пароля администратора. Если пароль еще не был изменен или есть необходимость в его повторном изменении, откройте приложение BlackArmor Manager (см. стр. 19). Пароль администратора можно изменить, выбрав пункт **Пароль администратора** в меню «Система». Пошаговые инструкции по обновлению пароля см. в интерактивной справочной системе по BlackArmor Manager.

Имя пользователя и пароль по умолчанию могут понадобиться в будущем, если настройки сервера будут сброшен до исходного состояния.

- Настройка **Global Access** – по умолчанию сервер BlackArmor недоступен из Интернета. Включите Seagate Global Access, если будет необходим доступ к файлам на сервере BlackArmor из любого места в мире или если необходимо предоставить доступ к своим файлам пользователям, находящимся а пределами локальной сети, таким как бизнес-клиенты или друзья (см. стр. 23).
- **Настройки Downloader** – по умолчанию сервер BlackArmor позволяет загружать большие файлы из Интернета в любое время с помощью инструмента BlackArmor Manager Downloader. С помощью BlackArmor Manager можно ограничить размер и число одновременных загрузок из Интернета, а также ограничить загрузки из Интернета определенными днями и часами (см. стр. 40).
- **Настройки мультимедийного сервера** – по умолчанию сервер BlackArmor не настроен как мультимедийный сервер. С помощью BlackArmor Manager можно сделать сервер мультимедийным для предоставления общего доступа к цифровым фотографиям, видео и музыке пользователям в локальной сети, а также включить службу iTunes, чтобы пользователи BlackArmor могли слушать потоковую музыку прямо на компьютере с установленным приложением iTunes (см. стр. 26).

УправлениеBlackArmor томами, общедоступными ресурсами и хранилищем

В этом разделе обсуждаются следующие темы.

- Общее представление о томах и общедоступных ресурсах
- Работа с томами
- Работа с общедоступными ресурсами
- Установка ограничений пространства хранения для пользователей BlackArmor
- Определение льготного периода для превышения квот
- Управление загрузкой файлов из Интернета на сервер BlackArmor

Общее представление о томах и общедоступных ресурсах

По умолчанию на сервере BlackArmor содержится один том и два общедоступных ресурса, «Загрузка» и «Общий». *Том* – это пространство хранения данных, которое может состоять из одного или нескольких дисковых накопителей или только из одной части дискового накопителя. *Общедоступный ресурс* – это папка. Общедоступные ресурсы создаются на томах.

Том и общедоступные ресурсы по умолчанию подходят для типичного использования, поэтому можно сразу начать сохранение, обеспечение защиты и предоставление общего доступа к файлам. Однако администратор BlackArmor может также использовать BlackArmor Manager для создания дополнительных томов и общедоступных ресурсов на сервере BlackArmor, если необходимо разделить общее пространство хранения на несколько меньших частей, которые будут использоваться в различных целях.

Например, можно создать три тома для хранения различных типов данных:

- Том A: Бизнес-файлы
- Том B: Хранилище файлов резервного копирования
- Том C: Файлы мультимедиа

Затем можно создать одну или несколько папок (общедоступных ресурсов) на каждом томе для выполнения определенных задач.

- Том A: Бизнес-файлы
  - Общедоступный ресурс 1: Клиентские файлы
  - Общедоступный ресурс 2: Финансовые файлы
  - Общедоступный ресурс 3: Файлы отдела кадров
- Том B: Хранилище файлов резервного копирования
  - Общедоступный ресурс 1: Ежедневные резервные копии
  - Общедоступный ресурс 2: Ежемесячные резервные копии
- Том C: Файлы мультимедиа
  - Общедоступный ресурс 1: Музыкальные файлы
  - Общедоступный ресурс 2: Фотографии
  - Общедоступный ресурс 3: Видеофайлы

Работа с томами

По умолчанию доступное пространство на сервере BlackArmor предоставляется одному тому, защита которого обеспечивается массивом RAID 1.

Общее представление о массивах RAID

RAID (Redundant Array of Independent Disks – избыточный массив независимых дисков) является технологией, обеспечивающей избыточность системы хранения для защиты данных от сбоев накопителей и прочих неполадок.

Существует несколько уровней массивов RAID, которые отличаются друг от друга степенью предоставляемой защиты (а также способом предоставления избыточности) и количеством поддерживаемых дисковых накопителей.

По умолчанию на сервере BlackArmor предварительно настроена защита RAID 1, которая обеспечивает «зеркалирование» данных сервера, сохраняя точные копии на обоих накопителях.

В этой таблице объясняются различные уровни массивов RAID, поддерживаемые сервером BlackArmor.

Табл. 1. Поддерживаемые уровни RAID для томов

Уровень RAID для томов	Требуемое количество дисковых накопителей	Описание
RAID 0 (также известен как массив с чередованием)	2–4	Том, в котором данные распределены равными разделами (чередование) по дисковым накопителям. Том с чередованием не содержит избыточных данных и поэтому *не обеспечивает защиты данных*.
RAID 1 (также известен как зеркалирование)	2	Том, в котором один дисковые накопитель является зеркальным отображением другого накопителя (одни и те же данные сохраняются на обоих дисках). Обеспечивает защиту данных.
Составной том (также известен как JBOD)	1–4	Группа установленных на сервере дисковых накопителей, *не защищенная с помощью RAID.*

Seagate рекомендует вносить изменения в защиту сервера с помощью массивов RAID только тем пользователям, которые имеют знания и опыт работы с технологией RAID.

Создание новых томов

Администратор BlackArmor может создавать все общедоступные ресурсы на томе по умолчанию или создать дополнительные тома с помощью BlackArmor Manager. При создании тома можно указать следующие характеристики:

- размер тома;
- дисковые накопители, которые следует использовать;
- уровень массива RAID для защиты данных (см. стр. 36).

Можно использовать одни и те же дисковые накопители в нескольких томах, если на накопителях имеется достаточно свободного места. Например, можно использовать половину пространства на накопителях 1 и 2 для создания тома А, а вторую половину на тех же дисковых накопителях для создания тома Б.

Чтобы создать новый том, откройте BlackArmor Manager (см. стр. 19). Тома доступны в меню «Хранилище». Дополнительную информацию о томах, включая удаление и изменение томов, можно найти в разделе «Справка».

Работа с общедоступными ресурсами

Общедоступные ресурсы на сервере BlackArmor могут быть общими (открыты всем пользователям с некоторыми ограничениями) или личными (ограничены определенными учетными записями пользователей).

Администратор BlackArmor может создавать, изменять или удалять общедоступные ресурсы в любое время. Однако при удалении общедоступного ресурса теряются все хранившиеся в нем файлы. Удаляйте общедоступные ресурсы с сервера BlackArmor с осторожностью.

Личные общедоступные ресурсы

Личный общедоступный ресурс связан с одной учетной записью пользователя; к нему могут получить доступ только пользователи BlackArmor, имеющие на это разрешение. Личные общедоступные ресурсы защищены паролями. (Администратор BlackArmor может преобразовать личный общедоступный ресурс в общий ресурс, изменив настройки ресурса в BlackArmor Manager.)

Можно ограничить доступ к общедоступному ресурсу следующими способами.

- Предоставить доступ только определенным пользователям BlackArmor.
- Дать пользователям BlackArmor доступ только на чтение. Доступ *только на чтение* означает, что пользователь BlackArmor сможет просматривать файлы на общедоступном ресурсе, но не сможет изменять эти файлы или загружать на общедоступный ресурс новые файлы.

- Предоставить любому пользователю BlackArmor полный доступ к общедоступному ресурсу, что позволит пользователю сохранять файлы на общедоступном ресурсе и записывать на него резервные копии, изменять файлы на ресурсах и загружать любые файлы с общедоступного ресурса на подключенный к серверу компьютер или USB-накопитель (см. стр. 58).

Владелец общедоступного ресурса также может предоставлять другим пользователям доступ к некоторым или всем файлам на этом ресурсе, используя систему Global Access. См. стр. 29.

Примечание. Чтобы одновременно подключить несколько *личных* общедоступных ресурсов, для каждого личного общедоступного ресурса должны использоваться одни и те же учетные данные входа.

Личные общедоступные ресурсы создаются вместе с учетной записью пользователя BlackArmor. Чтобы создать частный общедоступный ресурс, откройте BlackArmor Manager (см. стр. 19). Учетные записи пользователей расположены в меню «Доступ».

Чтобы изменить разрешения общедоступного ресурса, используйте инструмент BlackArmor Manager (см. стр. 19). Разрешения общедоступного ресурса находятся в меню «Доступ».

Пошаговые инструкции по использованию BlackArmor Manager см. в интерактивной справочной системе.

Общие общедоступные ресурсы

Общие общедоступные ресурсы не имеют ограничений, поэтому пользователи BlackArmor могут подключать столько общих общедоступных ресурсов, сколько потребуется.

Чтобы создать общий общедоступный ресурс, используйте BlackArmor Manager (см. стр. 19). Общедоступные ресурсы расположены в меню «Хранилище». Пошаговые инструкции по использованию BlackArmor Manager см. в интерактивной справочной системе.

Специальные функции общедоступных ресурсов

Эти функции доступны для любого общедоступного ресурса. Можно включить или отключить их для каждого ресурса.

- **Поддержка файловых протоколов** – общий доступ по сети к файлам с разных компьютеров возможен благодаря использованию стандартных файловых протоколов. Можно определить для каждого общедоступного ресурса любой из перечисленных ниже протоколов (в том числе все протоколы).
  - **CIFS (**Common Internet File System) – файловая система, которая позволяет пользователям разных компьютеров, работающих под управлением ОС Windows, совместно использовать файлы без необходимости установки специального программного обеспечения.

  - **FTP** (File Transfer Protocol) – обеспечивает безопасную передачу файлов через сеть Интернет между сервером BlackArmor и другими компьютерами.
  - **NFS** (Network File System) – обеспечивает общий доступ к файлам между компьютерами, работающими под управлением операционных систем Linux или UNIX, или компьютерами, на которых установлено клиентское программное обеспечение NFS.
- **Корзина** – можно защитить файлы на общедоступном ресурсе, включив корзину в приложении BlackArmor Manager. При включении корзины для общедоступного ресурса приложение BlackArmor Manager начнет сохранять файлы, удаленные с общедоступного ресурса, чтобы при необходимости их можно было восстановить.
- **Перетаскивание и сортировка** – можно определить для общедоступного ресурса автоматическую загрузку файлов мультимедиа в определенно место на компьютерах пользователей BlackArmor в зависимости от типа загружаемого файла. Например, загруженные музыкальные файлы будут автоматически сохраняться в папку «Музыка».

Чтобы включить или отключить любые из этих специальных функций, откройте BlackArmor Manager (см. стр. 19). Общедоступные ресурсы расположены в меню «Хранилище». Пошаговые инструкции по использованию BlackArmor Manager см. в интерактивной справочной системе.

Установка ограничений пространства хранения для пользователей BlackArmor

По умолчанию на сервере BlackArmor отсутствуют ограничения на пользовательское пространство хранения (исключением является размер тома, который задается для пользователя).

Однако администратор BlackArmor может определить ограничения для любой пользовательской учетной записи или общедоступного ресурса. Можно также задавать различные ограничения для каждой пользовательской учетной записи или для каждого общедоступного ресурса, к которому пользователь имеет доступ, а также задавать ограничения для определенных учетных записей пользователей.

Если пользователь BlackArmor заполняет выделенное ему пространство хранения, администратор BlackArmor должен удалить старые и ненужные файлы, чтобы освободить место для новых файлов.

Чтобы задать ограничения свободного места для пользователей BlackArmor, откройте BlackArmor Manager (см. стр. 19). Ограничения пространства хранения задаются для каждого тома на странице «Квота», которая находится в меню «Хранилище». Пошаговые инструкции по использованию BlackArmor Manager см. в интерактивной справочной системе.

Определение льготного периода для превышения квот

Администратор BlackArmor может задавать льготный период времени, в течение которого квота может превышать ограничение пространства хранения. Если квота достигнута, вы можете временно выделить дополнительные 100 МБ пространства хранения. Это даст пользователям достаточно времени для определения файлов, которые следует сохранить, а также для экономии свободного пространства.

Как только дата льготного периода достигнута, никакие дополнительные файлы не могут быть добавлены до тех пор, пока пространство не станет доступно.

Чтобы задать льготный период для сохраненных файлов, откройте BlackArmor Manager (см. стр. 19). Ограничение льготного времени задается на странице «Квота», которая находится в меню «Хранилище». Дополнительную информацию можно найти в интерактивной справочной системе по BlackArmor Manager.

Управление загрузкой файлов из Интернета на сервер BlackArmor

BlackArmor Manager содержит специальный инструмент для загрузки больших файлов на сервер с серверов FTP и других сайтов в Интернете. Этот инструмент называется Downloader. С его помощью администраторы BlackArmor могут управлять временем выполнения загрузок из Интернета, чтобы облегчить нагрузку на сервер.

При использовании инструмента Downloader задания загрузки из Интернета размещаются в очереди и автоматически выполняются в последовательности размещения. Если задание не располагается первым в списке, оно не будет начато сразу же при запуске инструмента. Администратор BlackArmor может изменять последовательность объектов в очереди, чтобы повысить приоритет определенных задач.

Можно ограничить время выполнения заданий загрузки из Интернета и количество одновременно выполняемых задач (не более трех). Загрузки из Интернета можно ограничить только вечерним временем, выходными и другим временем в течение недели, когда нагрузка на пропускную способность становится минимальной.

Оцените доступную для сервера BlackArmor пропускную способность и определите, какую ее часть можно выделить под длительные загрузки, затем ограничьте одновременную загрузку больших файлов или загрузку в пиковое время нагрузки на сервер BlackArmor.

Чтобы изменить настройки Downloader на сервере BlackArmor, проверить очередь Downloader и изменить приоритеты существующих заданий, откройте BlackArmor Manager (см. стр. 19). Управление инструментом Downloader выполняется в меню «Хранилище». Пошаговые инструкции по использованию BlackArmor Manager см. в интерактивной справочной системе.

Управление пользователями BlackArmor

В этом разделе описываются функции учетных записей пользователей, а также объясняется, как создавать новы учетные записи с помощью BlackArmor Manager. Пошаговые инструкции по использованию BlackArmor Manager см. в интерактивной справочной системе.

Работа с учетными записями пользователей

Каждый пользователь сервера BlackArmor нуждается в уникальной учетной записи пользователя. Однако учетная запись пользователя не требуется в то случае, если папка является общей и доступна всем пользователям. Администратор BlackArmor может настраивать каждую учетную запись пользователя в соответствии с нуждами этого пользователя BlackArmor. (Дополнительные сведения см. в разделе «Создание учетных записей пользователей» на стр. 22.)

Можно изменить следующее.

- Предоставление пользователю BlackArmor прав администратора
- Добавление пользователя в учетную запись группы (см. следующий раздел)
- Создание личного общедоступного ресурса для пользователя

После создания учетную запись пользователя можно в любое время изменить или удалить.

Чтобы создать, изменить или удалить учетную запись пользователя, используйте BlackArmor Manager (см. стр. 19). Учетные записи пользователей расположены в меню «Доступ». Пошаговые инструкции по использованию BlackArmor Manager см. в интерактивной справочной системе.

Создание и изменение групп пользователей

Можно упростить управление доступом к общедоступным ресурсам путем сортировки пользователей BlackArmor по группам. Учетные записи групп позволяют без труда задавать условия доступа к общедоступным ресурсам путем централизованного определения уровней доступа для отдельных пользователей или для целых групп пользователей.

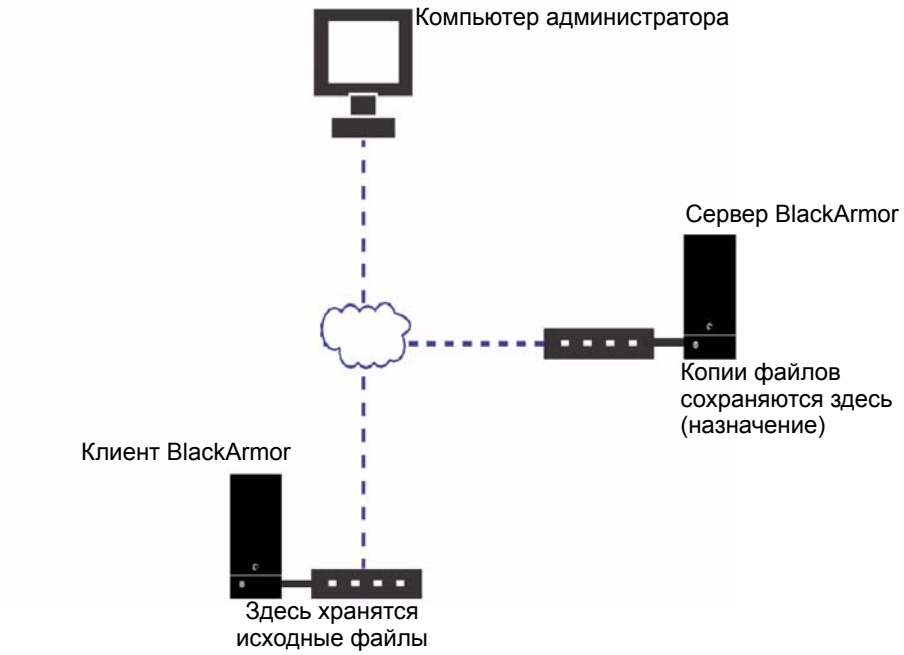
Группы пользователей в BlackArmor Manager можно создавать путем создания учетной записи группы и добавления в нее пользователей. Назначайте пользователей BlackArmor в группы, основываясь на общих потребностях в доступе.

При изменении разрешений доступа к общедоступным ресурсам на сервере BlackArmor можно назначить для группы определенный уровень доступа вместо назначения прав доступа для каждого пользователя по отдельности.

Чтобы создать, изменить или удалить учетную запись группы, откройте BlackArmor Manager (см. стр. 19). Группами можно управлять в меню «Доступ». Пошаговые инструкции по использованию BlackArmor Manager см. в интерактивной справочной системе.

Защита файлов BlackArmor с помощью резервного копирования по сети

Можно настроить резервное копирование с одного сервера NAS на другой, если между сервером BlackArmor и другим сервером в локальной сети установлено постоянное подключение и настроено автоматическое постоянное резервное копирование сервера BlackArmor. Это постоянное резервное копирование обеспечивает наилучшую защиту от потери данных или самого устройства, особенно если второй сервер расположен не в том же здании или части города (страны), где расположен сервер BlackArmor.



Используйте BlackArmor для настройки сетевого подключения между двумя серверами: клиентом BlackArmor (на нем хранятся файлы пользователей BlackArmor) и сервером BlackArmor (куда сохраняются копии или реплики файлов), затем начните исходное резервное копирование. После этого BlackArmor Manager можно использовать для определения расписания повторного резервного копирования.

Чтобы создать резервную копию сервера BlackArmor® на другом сервере в сети, следует сначала включить службу резервного копирования.

1. Откройте BlackArmor Manager (см. стр. 19).
2. На панели меню выберите **Хранилище**, а затем щелкните **Backup Manager**.
3. В меню **Хранилище** с левой стороны окна щелкните **Настройка сервера**.
4. Установите флажок рядом с параметром **Служба резервного копирования**.

Будут отображены сведения для проверки подлинности. Эти сведения используются при восстановлении резервных копий файлов.

5. Введите имя и пароль для проверки подлинности каждого псевдонима.
6. Выберите том устройства хранения.
7. Введите псевдоним, а затем щелкните **Добавить новый псевдоним**.
8. Нажмите кнопку **Отправить**.

Настройки сохранены.

Дополнительная информация о доступных типах задач резервного копирования содержится в интерактивной справочной системе по BlackArmor Manager.

Настройка сервера BlackArmor в качестве мультимедийного сервера

На сервере BlackArmor можно сохранять фотографии, видео и музыку для предоставления другим пользователям доступа к этому содержимому.

С помощью BlackArmor можно сделать сервер мультимедийным и определить автоматическую загрузку файлов мультимедиа в папки по умолчанию. Например, если пользователь загрузил музыкальные файлы, они будут автоматически сохранены в пользовательской папке «Музыка».

Можно также преобразовать сервер BlackArmor в сервер iTunes, чтобы пользователь BlackArmor мог слушать потоковую музыку прямо на компьютере с установленным приложением iTunes или на устройстве iPod, подключенном к компьютеру в сети.

Чтобы настроить сервер BlackArmor в качестве мультимедийного сервера, откройте BlackArmor Manager (см. стр. 19) и перейдите в меню «Мультимедиа». Пошаговые инструкции по использованию BlackArmor Manager см. в интерактивной справочной системе.

Отслеживание состояния сервера BlackArmor

Приложение BlackArmor Manager и сам сервер BlackArmor предоставляют различные способы наблюдения и отслеживания действий сервера и его состояния.

- Отслеживание состояния с помощью индикаторов сервера
- Использование предупреждений электронной почты для мониторинга состояния сервера
- Проверка состояния дискового накопителя с помощью SMART

Отслеживание состояния с помощью индикаторов сервера

Сервер BlackArmor имеет три светодиодных индикатора, которые помогают отслеживать состояние компонентов сервера. (Расположение индикаторов приведено на стр. 10.)

Табл. 2. Индикаторы передней и задней панелей

Индикатор	Состояние и цвет	Значение
Индикаторы на передней панели		
Питание	Непрерывный синий	Сервер включен
	Не горит	Сервер выключен
Состояние системы	Непрерывный синий	Сервер готов к использованию
	Мигающий синий	Сервер включается Выполняется перестройка тома RAID
	Непрерывный желтый	На сервере имеется системная ошибка, ошибка RAID или ошибка дискового накопителя
Состояние накопителя	Непрерывный синий	Накопитель готов к использованию
	Мигающий синий	Активность накопителя
Индикаторы на задней панели		
Порт локальной сети.	Не горит	Порт не подключен к сети
	Мигающий оранжевый (Л)	Активность подключения
	Зеленый (П)	Сетевое подключение

Отслеживание состояния сервера с помощью индикаторов

1. Индикатор состояния системы указывает на наличие проблемы. Голубой цвет означает, что сервер и его компоненты работают правильно.

Если индикатор состояния системы становится желтым, возникла проблема. Это может означать, что произошел сбой на накопителе.

2. Проверьте светодиодные индикаторы порта локальной сети на задней стороне сервера, чтобы убедиться в отсутствии неполадок с локальной сетью.

Если индикатор порта локальной сети не горит, сетевое подключение, возможно, не установлено. Сведения об устранении этой проблемы см. в «Устранение проблем» на стр. 61.

Использование предупреждений электронной почты для мониторинга состояния сервера

Примечание. Только администраторы BlackArmor могут определять предупреждения по электронной почте.

Можно использовать BlackArmor для уведомления администратора по электронной почте об изменении состояния сервера или об изменении какой-либо настройки сервера. Приложение BlackArmor Manager может отправлять предупреждения по электронной почте не более чем пяти пользователям. Для получения сообщений электронной почты необходимо иметь учетную запись Seagate Global Access.

Чтобы настроить предупреждения по электронной почте, используйте BlackArmor Manager (см. стр. 19). Предупреждения по электронной почте определяются в меню «Система». Пошаговые инструкции по использованию BlackArmor Manager см. в интерактивной справочной системе.

Проверка состояния дискового накопителя с помощью SMART

Примечание. Только администраторы BlackArmor могут выполнять диагностику SMART.

Можно использовать BlackArmor для выполнения диагностики SMART на дисковых накопителях сервера.

SMART – это технология самостоятельного анализа и отчетности, которая встраивается в дисковые накопители для автоматического отслеживания собственного состояния и предоставления отчетов о возможных проблемах.

Регулярное выполнение диагностики SMART на дисковых накопителях сервера поможет предотвратить сбой диска путем профилактического выявления неполадок. Так как в BlackArmor Manager можно протестировать только дисковые накопители, поддерживающие технологию SMART, следует всегда использовать в сервере только такие диски.

Чтобы выполнить диагностику SMART, откройте BlackArmor Manager (см. стр. 19). Тесты SMART располагаются в меню «Система». Пошаговые инструкции по использованию BlackArmor Manager см. в интерактивной справочной системе.

Изменение расширенных настроек сервера BlackArmor

В этом разделе описываются некоторые настройки сервера, которые можно изменять в соответствии с текущими потребностями.

Примечание. В особо отмеченных местах этого руководства описываемые изменения настроек сервера должны предпринимать только те пользователи, которые обладают знаниями в области соответствующих технологий.

В этом разделе обсуждаются следующие темы.

- Настройки динамической системы DNS
- Настройка файловых протоколов
- Настройки протокола NTP
- Настройки пониженного энергопотребления
- Настройки SSL
- Настройки бесперебойного источника питания (ИБП)
- Настройки протоколов веб-доступа
- Настройки рабочих групп и доменов

Настройки динамической системы DNS

Примечание. Изменять эти настройки следует только тем пользователям, которые знакомы с динамической системой DNS.

Динамическая система DNS – это способ поддержки связи между неизменным именем домена (например, www.seagate.com) и постоянно изменяющимся IP-адресом компьютера, который выдается сервером DHCP, а не указывается статически. Служба DDNS отслеживает изменение IP-адресов и перенаправляет весь сетевой трафик, предназначенный для вашего имени домена, на текущий IP-адрес.

Динамическую систему DNS на сервере BlackArmor можно настроить с помощью BlackArmor Manager. В BlackArmor Manager необходимо выбрать одного поставщика службы DNS, затем задать имя домена для этого сервера. Дополнительную информацию см. на веб-сайте выбранного поставщика службы DNS.

Чтобы настроить DDNS, откройте BlackArmor Manager (см. стр. 19). Настройки динамической системы DNS находятся в меню «Сеть». Пошаговые инструкции по использованию BlackArmor Manager см. в интерактивной справочной системе.

Настройка файловых протоколов

Общий доступ по сети к файлам с разных компьютеров возможен благодаря использованию стандартных файловых протоколов. Информация о поддерживаемых протоколах находится в разделе «Специальные функции общедоступных ресурсов» на стр. 38.

Настройки протокола NTP

Сервер времени NTP служит для синхронизации даты и времени на сервере BlackArmor. Служба NTP постоянно работает и изменяет время на сервере BlackArmor в соответствии с часами на сервере времени NTP.

Можно включить службу NTP на сервере BlackArmor, указав полное доменное имя или IP-адрес сервера времени NTP. Чтобы настроить службу NTP, откройте BlackArmor Manager и выберите пункт **Общая настройка** в меню «Система». Дополнительная информация содержится в интерактивной справочной системе.

Настройки пониженного энергопотребления

По умолчанию дисковые накопители на сервере BlackArmor постоянно вращаются при включенном электропитании сервера, однако в определенное время, например вечером, в выходные и праздники, сервер может не использоваться.

Чтобы сэкономить электроэнергию можно воспользоваться функцией снижения электропотребления в BlackArmor, которая работает путем *остановки* накопителей и перехода в режим ожидания при отсутствии обращения к накопителям. Пониженное энергопотребление можно включить в меню «Система» на странице **Дополнительно**.

Настройки SSL

Примечание. Добавление SSL в настройки сервера BlackArmor должно осуществляться только теми пользователями, которые знакомы с принципами работы SSL.

SSL (также TLS) – это тип шифрования, который используется для защиты данных, передаваемых по сети или через Интернет. SSL использует систему ключей, например секретные пароли, для обеспечения защищенной передачи и получения файлов. Дополнительные сведения см. в разделе «Настройки протоколов веб-доступа» на стр. 48.

Добавить поддержку SSL в настройки сервера BlackArmor можно, указав сертификат SSL и пару ключей.

Настройки бесперебойного источника питания (ИБП)

Бесперебойный источник питания – это источник питания, оснащенный аккумулятором. Последний позволяет компьютеру или серверу работать даже в случае перебоя в электропитании.

ИБП обеспечивает достаточно питания для того, чтобы можно было сохранить любые файлы, над которыми работает пользователь, и надлежащим образом отключить компьютер или сервер. Но это не означает, что любая система будет работать при сбое питания.

Сервер BlackArmor можно подключить к ИБП и указать настройки ИБП в BlackArmor Manager. Можно указать, через какое время ИБП отключит электропитание сервера BlackArmor на случай, если рядом не будет администратора. Можно определить следующие параметры завершения работы сервера.

- Срок действия аккумулятора на источнике бесперебойного питания достигает 15% от полного заряда аккумулятора или становится равным 5 минутам и менее.

или

- После прекращения подачи электроэнергии прошло указанное количество времени. (Это количество времени можно определить вручную.)

Настройки протоколов веб-доступа

По умолчанию сервер BlackArmor поддерживает протокол веб-доступа HTTP. HTTP – это протокол передачи гипертекста, который является самым распространенным способом хранения в Интернете файлов и данных.

Можно настроить на сервере BlackArmor использование протокола HTTPS (HTTP по SSL), если на сервере уже используется SSL. (См. «Настройки SSL» на стр. 47.)

Настройки рабочих групп и доменов

По умолчанию сервер BlackArmor настроен как *рабочая группа*. Рабочая группа – это несколько компьютеров, использующих общие ресурсы. Можно добавить любой компьютер в рабочую группу сервера или добавить сервер в существующую рабочую группу.

Кроме того, можно настроить сервер BlackArmor в качестве члена *домена*. Домен – это группа компьютеров, администрируемых централизованно как единое целое.

При добавлении сервера BlackArmor в качестве члена домена становится возможным централизованное управление сервером с контроллера домена Windows, что обеспечивает дополнительный уровень безопасности пользовательского доступа на сервер. Пользователи домена имеют собственные уникальные учетные записи и должны пройти аутентификацию для получения доступа к ресурсам.

Администратор домена должен авторизовать сервер BlackArmor в качестве члена домена. Чтобы добавить сервер в доен, необходимо знать имя пользователя и пароль администратора домена. Инструкции по добавлению сервера в качестве члена домена можно найти в интерактивной справочной системе по BlackArmor Manager.

Обслуживание сервера BlackArmor

В этом разделе объясняются базовые принципы надлежащего обслуживания сервера BlackArmor.

В этом разделе обсуждаются следующие темы.

- Меры безопасности при использовании оборудования и его обслуживания
- Поддержка микропрограммного обеспечения сервера в надлежащем состоянии
- Сброс настроек на сервере BlackArmor

Меры безопасности при использовании оборудования и его обслуживания

Придерживайтесь следующего руководства для поддержания сервера BlackArmor в работоспособном состоянии. В противном случае возможно снижение производительности или потеря данных.

- Всегда выключайте и перезапускайте сервер с помощью приложения BlackArmor Manager (инструкции содержатся в интерактивной справочной системе по BlackArmor Manager) или путем нажатия кнопки питания, расположенной на передней панели сервера. Не следует завершать работу сервера, выдергивая шнур из розетки или отключая питание на самом сервере.
- Сервер должен стоять на плоской, ровной поверхности. Сервер должен охлаждаться, на него не должна попадать влага, ничего не должно блокировать отверстия вентиляции во избежание перегрева.
- Вытирайте внешние поверхности сервера только сухой тряпкой (не используйте очистители любого типа), перед протиранием сервера выключите его из розетки, чтобы избежать поражения электрическим током.
- Не пытайтесь открыть сервер или снять его защитный корпус. Обратитесь в службу технической поддержки Seagate о адресу www.seagate.com/support, чтобы получить сведения о замене накопителей.
- Никогда не отключайте одновременно более одного накопителя. Это может привести к потере данных.

- В следующих случаях следует вызвать специалиста технической поддержки.
  - Шнур питания сервера поврежден.
  - На сервер была пролита жидкость, или он находится в прямом контакте с водой.
  - Сервер был уронен, или защитный корпус был поврежден.
  - Сервер не работает должным образом, несмотря на то что инструкции по эксплуатации всегда выполнялись правильно.

Поддержка микропрограммного обеспечения сервера в надлежащем состоянии

Примечание. Микропрограммное обеспечение сервера может обновлять только администратор BlackArmor.

Необходимо обновлять *микропрограмму* сервера (особенно встроенное в сервер программное обеспечение) по мере выхода новых версий. Это позволит использовать самые последние функции и возможности сервера. Новые версии микропрограммного обеспечения BlackArmor можно найти на веб-сайте Seagate www.seagate.com.

В BlackArmor Manager можно выбрать один из двух методов обновления.

- **Автоматические обновления микропрограммного обеспечения** – BlackArmor Manager загружает новое микропрограммное обеспечение, выполняет обновление и перезапускает сервер. Можно запустить обновление сразу же после загрузки или запланировать его на более удобное время.

В BlackArmor Manager можно также настроить регулярную проверку на наличие новых версий микропрограммного оборудования с последующим уведомлением администратора о наличии новой версии или ее немедленной установкой.

- **Обновление микропрограммы вручную** – необходимо проверять веб-сайт Seagate по адресу www.seagate.com на наличие новых версий микропрограммного обеспечения, загружать файлы микропрограмм и самому запускать обновление.

Seagate рекомендует использовать автоматическое обновление, чтобы обеспечить постоянное наличие на сервере самой последней версии микропрограммного обеспечения BlackArmor.

Сброс настроек на сервере BlackArmor

Ниже приведены шаги, которые необходимо выполнить для сброса имени сервера BlackArmor, настроек DHCP (режим сети) пароля для входа.

Примечание. Для выполнения этой задачи понадобится скрепка или другой узкий инструмент.

1. Любые действия на задней панели сервера должны выполняться с осторожностью.
2. Убедитесь, что сервер работает и подключен к локальной сети.
3. Найдите на задней панели сервера маленькое отверстие. Кнопка сброса находится внутри отверстия.
4. Вставьте конец скрепки в отверстие, затем нажмите и удерживайте кнопку сброса. *Не отпускайте* нажатую кнопку некоторое время.
5. Удерживайте кнопку сброса нажатой, пока светодиодный индикатор состояния системы на передней панели сервера не начнет мигать. Это займет несколько секунд.
6. Отпустите кнопку сброса.

Сервер автоматически перезагрузится. Процедура сброса завершается после перезапуска сервера и включения индикаторов на передней панели. Именем сервера становится BA-*MAC-адрес*, где *MAC-адрес* – это последние шесть знаков MAC-адреса сервера.

5. Рекомендации для пользователей BlackArmor®

- Введение
- Общее представление об учетной записи пользователя BlackArmor
- Доступ к общедоступным ресурсам и файлам на сервере BlackArmor
- Резервное копирование файлов
- Получение доступа к файлам BlackArmor через Интернет
- Загрузка больших файлов из сети Интернет на сервер BlackArmor
- Извлечение удаленных файлов из корзины

Введение

В этой главе содержатся рекомендации и сведения, которые помогут пользователям BlackArmor® полноценно использовать сервер BlackArmor.

Пользователи BlackArmor могут выполнять следующие действия.

- Хранить свои файлы на сервере BlackArmor и предоставлять к ним общий доступ другим пользователям.
- Создавать резервные копии файлов, приложений и даже операционных систем с помощью приложения BlackArmor Backup.
- Пользоваться веб-доступом к файлам на сервере BlackArmor с помощью службы Global Access (если включена).
- Загружать большие веб-файлы напрямую из Интернета и сохранять их на сервере BlackArmor, используя приложение BlackArmor Manager Downloader.
- Восстанавливать случайно удаленные файлы из корзины BlackArmor Manager (если включена).

Общее представление об учетной записи пользователя BlackArmor

В этом разделе описываются функции и возможные ограничения учетной записи пользователя BlackArmor.

Ограничения доступа

Общедоступные ресурсы на сервере BlackArmor могут быть общими (открыты всем пользователям с некоторыми ограничениями) или личными (ограничены определенными учетными записями пользователей).

Обратитесь к администратору сервера BlackArmor, чтобы узнать об имеющихся у вас ограничениях доступа.

Личные общедоступные ресурсы

Личные общедоступные ресурсы защищаются паролем, их использование ограничено только теми пользователями, которых определил администратор BlackArmor.

После создания администратором BlackArmor учетной записи пользователя можно ограничить доступ к личному общедоступному ресурсу следующим образом:

- ограничив доступ к этому общедоступному ресурсу только для определенных пользователей BlackArmor.
- дать пользователям BlackArmor доступ только на чтение. Доступ *только на чтение* означает, что пользователь сможет просматривать файлы на общедоступном ресурсе, но не сможет изменять эти файлы или загружать на общедоступный ресурс новые файлы.

Пользователь имеет полный доступ к своему личному общедоступному ресурсу, что позволяет сохранять и создавать резервные копии файлов прямо на общедоступном ресурсе, изменять эти файлы, а также загружать любые фалы с общедоступного ресурса на свой компьютер или на USB-накопитель, подключенный к серверу (см. стр. 58).

Можно предоставить другим пользователям доступ ко всем или некоторым файлам на личном общедоступном ресурсе как в локальной сети, так и из Интернета с помощью службы Global Access. Дополнительную информацию и инструкции по настройке учетной записи Global Access см. на стр. 29. В инструкциях пользователя Global Access указано, как предоставлять доступ к файлам другим пользователям.

Примечание. Чтобы одновременно подключить несколько *личных* общедоступных ресурсов, для каждого личного общедоступного ресурса должны использоваться одни и те же учетные данные входа.

Общие общедоступные ресурсы

Общие общедоступные ресурсы не имеют ограничений, поэтому пользователи могут подключать столько общих общедоступных ресурсов, сколько потребуется.

Ограничения пространства хранения

Администратор BlackArmor может ограничивать объем пространства хранения, предоставляемого для определенного общедоступного ресурса.

Пространство может быть ограничено для одного общедоступного ресурса, однако другой ресурс не будет иметь ограничений; для одного общедоступного ресурса может быть задан больший объем, чем для другого. Или можно вообще не вводить ограничений пространства за исключением максимального пространства хранения на самом сервере BlackArmor.

Сведения об ограничениях пространства хранения может предоставить администратор BlackArmor.

Если вы заполнили выделенное пространство хранения, следует удалить старые или ненужные файлы для освобождения места или обратиться к администратору BlackArmor для предоставления дополнительного пространства.

Автоматическая сортировка файлов мультимедиа

Общедоступные ресурсы на сервере BlackArmor могут быть настроены для автоматической сортировки файлов с целью помещения их в определенные папки на компьютере, основываясь на типах файлов. Например, загруженные музыкальные файлы будут автоматически сохраняться в папку «Наша музыка».

О наличии функции автоматической сортировки (в BlackArmor Manager эта функция называется перетаскиванием и сортировкой) можно узнать у администратора BlackArmor.

Ограничения льготных периодов для квот

При наличии квоты хранения для учетной записи администратор BlackArmor может задать льготный период, в течение которого квота сможет превышать ограничения хранения. Как только дата льготного периода достигнута, никакие дополнительные файлы не могут быть добавлены до тех пор, пока пространство не станет доступно.

О наличии льготных периодов для хранения файлов на сервере можно узнать у администратора BlackArmor.

Поддержка общедоступными ресурсами файловых протоколов

Компьютеры получают доступ к файлам в сети с помощью стандартных файловых протоколов. Информация о поддерживаемых протоколах находится в разделе «Специальные функции общедоступных ресурсов» на стр. 38.

Доступ к общедоступным ресурсам и файлам на сервере BlackArmor

После подключения к серверу BlackArmor и подключения или привязки общедоступных ресурсов можно начать сохранение файлов на сервере.

Примечание. Можно подключать или привязывать столько общих и личных общедоступных ресурсов, сколько потребуется. Однако, чтобы одновременно подключить несколько *личных* общедоступных ресурсов, для каждого личного общедоступного ресурса должны использоваться одни и те же учетные данные входа.

Доступ к общедоступным ресурсам на сервере BlackArmor можно получить следующим образом:

- локально – точно так же, как открывается любой сетевой диск на компьютере (например, с помощью Windows Explorer). Справку по подключению или привязке общедоступных ресурсов к компьютеру см. на стр. 28.
- удаленно, через Интернет, с помощью Seagate Global Access (если администратор BlackArmor включил службу Global Access на сервере BlackArmor). Дополнительную информацию о службе Global Access см. на стр. 29.

После успешного подключения к общедоступному ресурсу можно просматривать и загружать файлы с общедоступного ресурса, а также выкладывать файлы и резервные копии на этот ресурс при наличии соответствующих разрешений (см. стр. 54).

Администратор BlackArmor может оказать помощь в получении доступа к нужным общедоступным ресурсам и объяснить общую концепцию прав на просмотр, загрузку и запись.

Резервное копирование файлов

Чтобы защитить импортированные файлы от потери, повреждения или случайного удаления, необходимо постоянно выполнять резервное копирование файлов с помощью приложения BlackArmor Backup.

Можно также создавать резервные копии файлов, загружая их с сервера BlackArmor на внешний USB-накопитель или записывать их с USB-накопителя обратно на сервер.

Резервное копирование файлов с помощью BlackArmor Backup

BlackArmor Backup – это полноценное приложение для резервного копирования, оснащенное различными функциями, с помощью которых можно настроить систему резервного копирования в соответствии со своими требованиями.

Можно использовать BlackArmor Backup для запуска резервного копирования в любое время. Можно также использовать BlackArmor для настройки регулярного резервного копирования, которое будет выполняться в любое удобное время (например, ночью или в течение выходных, когда вы не используете свой компьютер).

Приложение BlackArmor Backup можно использовать для защиты всех файлов, приложений и даже операционных систем на компьютерах.

Если вы еще не установили BlackArmor Backup, инструкции по установке содержатся на стр. 28.

Дополнительную информацию можно получить в *руководстве пользователя BlackArmor Backup* или в интерактивной справочной системе.

Резервное копирование файлов между серверами

Примечание. Это действие может выполняться только администратором.

BlackArmor Manager можно использовать для сохранения резервных копий на сервер BlackArmor, а также для резервного копирования этого сервера на другой сервер в локальной сети. Чтобы выполнить резервное копирование на другой север, необходимо знать IP-адрес этого сервера и учетные данные для входа.

Backup Manager находится в меню «Хранилище» приложения BlackArmor Manager. Пошаговые инструкции по резервному копированию файлов между серверами можно найти в интерактивной справочной системе по BlackArmor Manager.

Резервное копирование с использованием внешнего USB-накопителя

Примечание. Это действие может выполняться только администратором.

Можно использовать BlackArmor Manager для незамедлительного резервного копирования файлов (или копирования по расписанию) *с* внешнего USB-накопителя *на* сервер BlackArmor или *с* сервера BlackArmor на внешний USB-накопитель.

Чтобы начать резервное копирование с использованием внешнего USB-накопителя, вставьте накопитель в порт USB (порт 2) на задней панели сервера BlackArmor (на стр. 11 показано расположение портов USB на сервере), затем откройте BlackArmor Manager (см. стр. 19). Приложение Backup Manager расположено в меню «Хранилище».

Пошаговые инструкции по резервному копированию файлов можно найти в интерактивной справке по BlackArmor Manager.

Получение доступа к файлам BlackArmor через Интернет

Если администратор BlackArmor включил на сервере службу Global Access, зарегистрируйтесь для получения бесплатной учетной записи Global Access, чтобы иметь возможность открывать файлы на сервере BlackArmor из сети Интернет.

Seagate Global Access – это служба, с помощью которой можно просматривать, загружать, предоставлять общий доступ и работать с файлами, хранящимися на сервере BlackArmor, из любой точки мира, предоставлять общий доступ к файлам, хранящимся на личном общедоступном ресурсе, или совместно использовать ваши файлы с любым пользователем, находящимся за пределами локальной сети.

С помощью Global Access можно выполнять следующие действия.

- Загружать важные бизнес-файлы или презентации из офиса клиента в любой точке земного шара.
- Предоставлять доступ к файлам клиентам, не требуя от них использования FTP-приложений.
- Загружать важные файлы с переносного компьютера на сервер, чтобы гарантировать их сохранность во время поездки.
- Предоставлять другим пользователям доступ к файлам на личном общедоступном ресурсе.

Чтобы получить доступ к серверу BlackArmor через Интернет, выполните следующие действия.

- Убедитесь, что включена глобальная служба Global Access на сервере BlackArmor. Дополнительную информацию можно получить у администратора BlackArmor.
- Создайте учетную запись Global Access. Любой пользователь, желающий получить доступ к серверу BlackArmor через Интернет должен иметь собственную учетную запись Global Access. (Учетные записи предоставляются бесплатно.)

Инструкции по созданию учетной записи Global Access см. на стр. 29. В инструкциях пользователя Global Access указано, как предоставлять доступ к файлам другим пользователям.

Загрузка больших файлов из сети Интернет на сервер BlackArmor

BlackArmor Manager содержит специальный инструмент для загрузки больших файлов на сервер с серверов FTP и других сайтов в Интернете. Этот инструмент называется **Downloader**. С его помощью администраторы BlackArmor могут управлять временем выполнения загрузок из Интернета, чтобы облегчить нагрузку на сервер.

Задания Downloader могут не начинаться немедленно. Загрузки из Интернета выполняются автоматически в том порядке, в котором они отображаются в очереди Downloader (очередь может редактироваться администратором BlackArmor), поэтому, если ваше задание не находится первым в списке, его загрузка не начнется сразу же после запуска Downloader.

Кроме того, администратор BlackArmor может задавать ограничения на время выполнения загрузок из Интернета и количество одновременных загрузок (никогда не превышает трех). Администраторы BlackArmor могут ограничивать время загрузки вечерами, выходными и другим временем в течение недели, когда нагрузка а пропускную способность является минимальной.

Информацию о времени загрузки файлов из Интернета с помощью Downloader можно получить у администратора BlackArmor. Кроме того, у администратора можно попросить переместить ваше задание вверх по списку загрузок Downloader.

Извлечение удаленных файлов из корзины

Общедоступные ресурсы на сервере BlackArmor могут быть защищены с помощью корзины BlackArmor Manager. При включении корзины для общедоступного ресурса приложение BlackArmor Manager начнет сохранять файлы, удаленные с общедоступного ресурса, чтобы при необходимости их можно было восстановить.

Если файл был случайно удален, откройте BlackArmor Manager (см. стр. 19) и щелкните пункт **Корзина**. Пошаговые инструкции по извлечению удаленных файлов см. в интерактивной справочной системе по BlackArmor Manager.

6. Устранение проблем

В этой главе представлены решения наиболее распространенных проблем, которые могут возникать при настройке и использовании сервера BlackArmor.

- Советы по устранению неполадок общего характера
- Распространенные проблемы и их решение

Советы по устранению неполадок общего характера

Если у вас есть проблемы с настройкой или использованием сервера BlackArmor, следуйте этим инструкциям.

- Убедитесь в том, что сервер надлежащим образом подключен к локальной сети. Убедитесь в том, что кабель Ethernet подключен и функционирует надлежащим образом.
- Убедитесь, что сеть функционирует надлежащим образом.
- Убедитесь в том, что сервер надлежащим образом подключен к источнику питания и включен. Убедитесь в том, что все дисковые накопители работают надлежащим образом.
- Убедитесь, что используемый компьютер соответствует системным требованиям BlackArmor. Дополнительные сведения см. в разделе «Системные требования» на стр. 8.
- Убедитесь, что на компьютере используется поддерживаемый веб-браузер. Список поддерживаемых браузеров приведен в разделе «Системные требования» на стр. 8.
- Убедитесь, что при входе вы вводите правильные имя администратора и пароль. (Помните, что пароли чувствительны к регистру!)

Распространенные проблемы и их решение

В этом разделе предоставляются решения распространенных проблем, которые могут возникнуть в BlackArmor Manager.

Я не могу подключиться к серверу по локальной сети.

Убедитесь, что сервер включен и подключен к сети.

Попытайтесь подключиться к серверу с другого компьютера.

Попытайтесь заменить кабель Ethernet.

Я не могу подключиться к серверу через Интернет.

Проверьте, включена ли на сервере возможность Global Access. См. «Предоставление доступа к BlackArmor с помощью службы Seagate Global Access» на стр. 23.

Настройте электронную почту в BlackArmor Manager, затем отправьте тестовое сообщение.

Я не могу открыть BlackArmor Manager.

Убедитесь, что сервер включен и подключен к сети. Запустите инструмент BlackArmor и попытайтесь подключиться к серверу, затем запустите BlackArmor Manager.

Я не могу войти в BlackArmor Manager.

Убедитесь в том, что вы вводите правильные имя пользователя и пароль. Помните, что имена пользователей и пароли зависят от регистра.

Я не могу получить доступ к общедоступному ресурсу.

Убедитесь, что у вас есть доступ к этому общедоступному ресурсу.

Убедитесь в том, что вы вводите правильные имя пользователя и пароль. Помните, что имена пользователей и пароли зависят от регистра.

Том, на котором находится общедоступный ресурс, может работать в пониженном режиме вследствие ошибки или неисправности дискового накопителя. Проверьте состояние дисковых накопителей на сервере; дополнительная информация содержится в разделе «Отслеживание состояния с помощью индикаторов сервера» на стр. 44.

Я не могу получить доступ к файлу на общедоступном ресурсе.

Убедитесь, что вы имеете доступ к этому файлу.

Том, на котором находится общедоступный ресурс, может работать в пониженном режиме вследствие ошибки или неисправности дискового накопителя. Проверьте состояние дисковых накопителей на сервере; дополнительная информация содержится в разделе «Отслеживание состояния с помощью индикаторов сервера» на стр. 44.

Я не могу сохранить файлы на общедоступном ресурсе, потому что соответствующий том переполнен.

Если вы являетесь рядовым пользователем, обратитесь к администратору BlackArmor.

Если вы являетесь администратором, рассмотрите возможность удаления некоторых файлов, хранящихся в настоящее время на сервере.

Не удалось выполнить обновление микропрограммного обеспечения.

Попытайтесь обновить микропрограммное обеспечение вручную. Для получения дополнительной информации обратитесь в службу технической поддержки Seagate по адресу www.seagate.com/support.

Том работает в пониженном режиме.

Возможно, произошел сбой дискового накопителя. Для получения дополнительной информации обратитесь в служу технической поддержки Seagate по адресу www.seagate.com/support.

Я не могу слушать потоковую музыку с сервера BlackArmor.

Убедитесь, что на компьютере установлено приложение iTunes. Убедитесь, что используется компьютер, подключенный к локальной сети. Убедитесь, что имеется доступ к общему ресурсу, где размещается музыка.

7. Технические спецификации

Сетевое подключение

- 1 сетевой разъем Ethernet RJ-45 10/100/1000

Порты USB

- 2 порта USB 2.0

Источник питания

- Внешний источник питания 36 Вт (весь диапазон переменного тока на входе, 12 В постоянного тока на выходе)

Дисковые накопители

- 2 дисковых накопителя SATA II

Физические размеры

- Высота: 200 мм
- Ширина: 118 мм
- Длина: 189 мм

Питание

- Номинальная мощность: 100–240 В переменного тока, 50–60 Гц
- Входное напряжение: 90–264 В переменного тока
- Устойчивый переменный ток: 1,5 А (среднеквадратический) при 100 В
- Диапазон частот на входе: 47–63 Гц

Условия эксплуатации

- 55–35 °C (41–95 °F)
- Влажность 20–80 % (неконденсирующаяся)

Условия в выключенном состоянии

- -20 – +60 °C (-20,00 – +60,00 °F)
- Влажность 20–80 % (неконденсирующаяся)

8. Глоссарий

CIFS

Common Internet File System. Файловая система, которая позволяет пользователям с разными компьютерами под управлением Windows совместно использовать файлы без необходимости установки специального программного обеспечения.

FTP

Протокол FTP. Формат для обмена файлами в Интернете. FTP обычно используется для загрузки файлов на сервер или с сервера через Интернет.

HTTP (Hypertext Transfer Protocol, протокол передачи гипертекста)

Правила для обмена данными в самой распространенной форме (гипертекстовых документов) по сети Интернет.

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, протокол передачи гипертекста через SSL)

Правила для обмена документами HTTP с использованием защищенных подключений.

IP-адрес

Идентификатор компьютера, сервера или другого устройства в сети TCP/IP. IP-адреса представляют собой комбинацию из четырех чисел, разделенных точками. (Например, 123.456.78.1.) Каждое устройство в локальной сети имеет уникальный IP-адрес.

JBOD

JBOD (просто группа накопителей). См. Составной том.

NFS

Файловая система NFS. Приложение, позволяющее всем пользователям в сети обмениваться файлами, которые хранятся на различных типах компьютеров.

RAID

Redundant Array of Independent Disks (Избыточный массив независимых дисков). Технология, которая объединяет дисковые накопители для повышения производительности и устойчивости к ошибкам (способности обеспечить целостность данных даже при выходе из строя дискового накопителя).

RAID 0

См. Чередование.

RAID 1

См. Зеркало.

RAID 5

Уровень защиты RAID. Том RAID 5 создается как минимум из трех дисковых накопителей и использует чередование данных и контроль четности для обеспечения избыточности. (Контроль по четности — это дополнительная информация, которая используется для воссоздания данных в случае отказа дискового накопителя. На томах с RAID 5 данные контроля по четности равномерно чередуются с хранящимися данными на всех дисковых накопителях.) Данные контроля по четности обеспечивают защиту данных, а чередование повышает производительность. См. также Чередование.

RAID 10

Уровень защиты RAID. Том RAID 10 создается из двух или нескольких томов RAID 1 одинакового размера. Для данных на томе с RAID 10 одновременно используются чередование и зеркальное отображение. Зеркальное отображение обеспечивает защиту данных, а чередование повышает производительность. См. также Зеркало и Чередование.

Seagate Global Access

Служба, позволяющая просматривать, загружать, предоставлять общий доступ и работать с файлами, которые хранятся на сервере BlackArmor, из любой точки мира. Кроме того, вы можете использовать службу Global Access для загрузки файлов на сервер BlackArmor.

SMART

Технология SMART. Встроенная в дисковые накопители технология, которая позволяет автоматически отслеживать их состояние и сообщать о возможных проблемах. Не все дисковые накопители поддерживают технологию SMART.

USB

Универсальная последовательная шина USB. Интерфейс между компьютером и устройствами USB, которые подключаются к компьютеру. Компьютер взаимодействует с устройствами USB посредством интерфейса USB.

USB-накопитель

Портативный дисковый накопитель, который подсоединяется к компьютеру с помощью кабеля USB вместо установки внутри самого компьютера. Также известен как флеш-накопитель или внешний жесткий диск USB.

Администратор

Администратор BlackArmor несет ответственность за сервер BlackArmor и все настройки. Администратор может настраивать или удалять учетные записи пользователей, группы и папки, присваивать или удалять уровни доступа, изменять любые параметры на сервере и назначать других администраторов. См. также Пользователь.

Внешний накопитель USB

См. USB-накопитель.

Домен

Группа компьютеров, администрируемых как единый блок из центрального местоположения.

Замена без выключения питания («горячая замена»)

Извлечение и замена дискового накопителя без предварительного отключения сервера от источника питания.

Зеркало

Уровень защиты RAID, также известный как RAID 1. Зеркало создается из двух дисковых накопителей, когда один из них является зеркальным отображением другого (на каждом дисковом накопителе хранятся одни и те же данные). П сравнению с независимыми дисковыми накопителями том с зеркальной копией обеспечивает более высокую производительность, но имеет в 2 раза меньшую емкость.

ИБП

Источник бесперебойного питания. Источник питания с батареей, которая некоторое время поддерживает работоспособность компьютера или сервера в случае сбоя питания. ИБП обеспечивает достаточно питания для того, чтобы можно было сохранить любые файлы, над которыми работает пользователь, и надлежащим образом отключить компьютер или сервер. Но это не означает, что любая система будет работать при сбое питания.

Ключ RSA

Криптографический алгоритм, который является частью SSL; вид шифрования, используемый для защиты данных, передаваемых по сети или Интернету. Алгоритм получил свое название по первым буквам имен ученых Райвеста, Шамира и Адельмана, которые изобрели данную технологию.

Контроль по четности

Данные создаются на томах с защитой RAID 5, которая используется для восстановления файлов в случае выхода из строя одного из дисковых накопителей сервера. См. также RAID 5.

Локальный доступ

Доступ к серверу с компьютера в локальной сети. Или ручной доступ к серверу, который подразумевает физический контакт с сервером или его кабелями. См. также Удаленный доступ.

Микропрограммное обеспечение

Программное обеспечение, встроенное в оборудование.

Общедоступный ресурс

Папка на сервере BlackArmor, которая хранит и защищает файлы резервного копирования, а также другие файлы, к которым могут иметь доступ другие пользователи.

Остановка вращения жесткого диска

Это понятие относится к дисковым накопителям и означает прекращение вращения жесткого диска.

Пользователь

В приложении BlackArmor Manager пользователь, который может сохранять, создавать резервные копии и предоставлять общий доступ к файлам с использованием сервера BlackArmor, но не может изменять учетные записи пользователей, учетные записи групп или настройки сервера.

Протокол доступа к сети

Правила передачи информации через Интернет. Сервер BlackArmor поддерживает два протокола доступа к сети: HTTP и HTTPS.

Рабочая группа

Группа компьютеров в сети, которые совместно используют ресурсы.

Резервное копирование архива

См. Ключ RSA.

Сервер

Компьютер или устройство в сети, которое осуществляет управление ресурсами. Сервер BlackArmor представляет собой файловый сервер, то есть устройство, которое предназначено для хранения файлов; он также может использоваться в качестве сервера печати, то есть устройства, которое управляет одним или несколькими принтерами.

Сервер NTP (Network Time Protocol)

Синхронизирует дату и время на компьютерах и серверах в сети на основе универсального времени.

Сертификат SSL

Сертификат Secure Socket Layer, часть метода шифрования SSL. SSL (также TLS) – это тип шифрования, который используется для защиты данных, передаваемых по сети или через Интернет. SSL использует систему ключей, например секретные пароли, для обеспечения защищенной передачи и получения файлов.

Событие

Проблема или изменение в настройках сервера BlackArmor. Изменение имени сервера или неисправность дискового накопителя являются примерами событий на сервере.

Составной том

Группа установленных на сервере дисковых накопителей, не защищенная с помощью RAID. Также этот режим использования накопителей известен как JBOD. См. также RAID.

Том

Пространство хранения данных, которое может состоять из одного или нескольких дисковых накопителей или только из части одного дискового накопителя.

Удаленный доступ

Доступ к серверу с компьютера, который находится за пределами локальной сети. Например, это может быть доступ к серверу с компьютера клиента через Интернет.

Удаленный доступ также может относиться к отключению или перезагрузке сервера с использованием BlackArmor Manager вместо физического нажатия на кнопку отключения питания. См. также Локальный доступ.

Уровень доступа

Известно также как уровень доступа, это пределы доступа любого пользователя на сервер BlackArmor®. BlackArmor Manager предоставляет два уровня разрешений: *администратор* и *пользователь*.

Учетная запись группы

В BlackArmor Manager учетные записи пользователей представлены в виде группы, с тем чтобы сделать управление доступом к папкам проще и быстрее. Все пользователи в группе имеют одинаковый уровень доступа к определенной папке. См. также Учетная запись пользователя.

Учетная запись пользователя

Учетная запись, имеющая имя пользователя и пароль, которую пользователь использует для получения доступа серверу BlackArmor. Учетные записи пользователя имеют уровни доступа, связанные с ними.

Форматирование

Под форматированием дискового накопителя подразумевается его подготовка к чтению и записи данных. Форматирование удаляет исходную информацию с дискового накопителя, проверяет его и подготавливает к использованию. Форматирование может привести к удалению существующих файлов на дисковом накопителе. Дисковые накопитель перед использованием должен быть отформатирован.

Частный общедоступный ресурс

Папка, доступная только пользователям, которым предоставлен доступ владельцем папки.

Чередование

Также этот режим известен как RAID 0. Том с чередованием включает два или несколько дисковых накопителей, на которых данные распределены равномерно (с чередованием) по всем дисковым накопителям блоками одинакового размера. Том с чередованием не содержит избыточных данных и поэтому *не обеспечивает защиты данных*.

Однако по сравнению с группой независимых друг от друга дисков одинакового размера том с чередованием обеспечивает более высокую производительность.

Указатель