ООО «НТК Интерфейс»

КОНЦЕНТРАТОР ТЕЛЕМЕТРИИ «ДЕЛЬТА ХР»

Особенности администрирования

Екатеринбург 2013

Оглавление

ВВЕДЕНИЕ

Концентратор телеметрии «Дельта XP» с выносным твердотельным диском и предустановленной операционной системой Windows 7 Embedded имеет ряд особенностей администрирования. Данный документ предназначен для ознакомления пользователей с этими особенностями.

1 НАЧАЛО РАБОТЫ

Для начала работы с концентратором требуется или подключить к нему монитор/консоль оператора, или, что более удобно, воспользоваться удаленным администрированием с помощью комплекса «Remote Manipulator System». Для этого на концентраторе установлена серверная часть программы, соответственно на удаленный компьютер, находящийся в той же подсети, требуется установить «Remote Manipulator System Viewer», указать ip-адрес концентратора (по умолчанию концентратору назначен адрес 192.168.0.1) и пароль программы (по умолчанию «admin-root», без кавычек). Подробное описание комплекса удаленного администрирования приведено в разделе 4 данного документа.

Получив любым из способов доступ к экрану концентратора, включаем его и ждем появления стартовой заставки Windows 7 Embedded. Появится окно с требованием ввода пароля. Логин по умолчанию «Admin», пароль — «root» (без кавычек). Обратите внимание, при запуске Windows запускает русскую раскладку (текущая раскладка отображается в левом верхнем углу стартового экрана), перед вводом пароля требуется переключиться на английскую раскладку, с помощью сочетания клавиш Shift+Alt.

После входа открывается стандартный рабочий стол Windows, концентратор готов к работе.

2 ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

В концентраторе используется расширенная система безопасности, запрещающая изменения любых файлов на диске, кроме файлов в заданных директориях.

Как работает защита: при любом изменении в файловой системе (будь то создание/редактирование файлов, редактирование настроек Windows и пр.), данное изменение записывается в локальный кэш, который очищается при перезапуске системы. Благодаря этому обеспечивается максимальная безопасность системы: при ошибочных действиях персонала или вирусной активности невозможно изменить параметры системы.

Управлений данной системой безопасности обеспечивается установленным приложением «FBWF Manager», ярлык которого вынесен на рабочий стол

концентратора. По умолчанию общий доступ к файловой системе закрыт, открытыми являются две директории: директория сервера «ОИК Диспетчер НТ» (C:/Program Files/InterfaceSSH) и временная директория для хранения файлов (C:/_Tmp).

В какие-то моменты может потребоваться внесение изменений в систему, например, изменить пароль для входа администратора, изменить ip-адрес концентратора и т.д. Для этого используется следующий алгоритм:

— С помощью ярлыка на рабочем столе запускается приложение «FBWF Manager»;

— В окне программы внутри поля Refresh Info выбирается пункт Next Session, затем снимается флаг с пункта Filter Enabled (см. рисунок 1). Данным действием мы сообщаем системе, что при следующей сессии работы (после перезагрузки) фильтрация записи будет отключена;

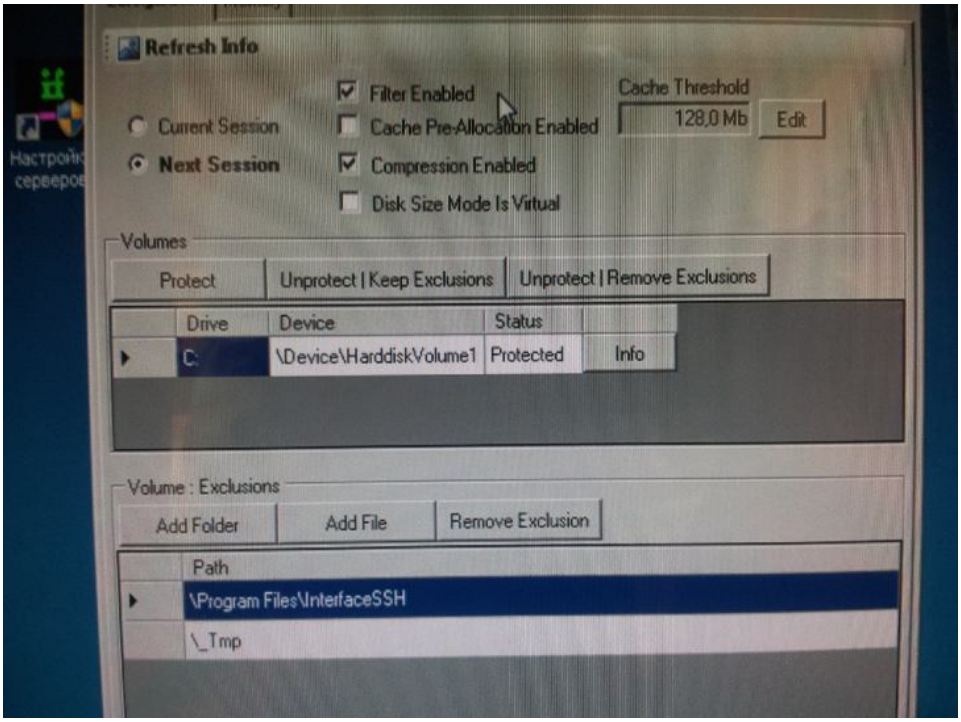

Рисунок 1 – окно программы «FBWF Manager»

— При необходимости корректно завершается работа сервера «ОИК Диспетчер НТ» и других запущенных программ. Перезагружается систему;

— После перезапуска вновь открывается приложение «FBWF Manager». Проверяется, чтобы в пункте Filter Enabled отсутствовал флаг;

— В систему вносятся необходимые изменения;

— Обязательно вновь перезагружается система;

— После перезапуска открывается приложение «FBWF Manager». Проверяется, чтобы в пункте Filter Enabled присутствовал флаг;

— Проверяются выполненные ранее изменения;

— Дальнейшие изменения в системе снова запрещены. При необходимости новых изменений данный алгоритм повторяется.

Обратите внимание, для изменения конфигурации сервера «ОИК Диспетчер НТ» данные действия выполнять не нужно. Директория сервера добавлена в исключения, что позволяет выполнять перезапись конфигурации. Однако следует учитывать две особенности сервера для данной системы безопасности:

1 По умолчанию на сервере телеметрии установлена специальная внешняя задача программы «FBWF Manager», обеспечивающая конкретную фильтрацию записи при перезагрузке после внесения изменений по указанному выше алгоритму. Данная внешняя задача не рекомендуется к отключению. В противном случае потребуется вручную устанавливать фильтр для запрета записи даже после второй перезагрузки;
2 Поскольку информация об автозапуске сервера «ОИК Диспетчер НТ» указывается в системных настройках, а не в рабочем каталоге, для сохранения настроек автоматического или ручного запуска сервера потребуется временно отключить фильтрацию согласно указанному выше алгоритму.

3 АВАРИЙНОЕ ВОССТАНОВЛЕНИЕ СИСТЕМЫ

Для целей резервного и аварийного восстановления системы рекомендуется сразу после окончания наладки произвести резервное копирование системного диска любой удобной для пользователя программой резервирования. Единственное требование к программе резервного копирования – умение восстанавливать начальное смещение файловой системы. В данном случае для SSD – 1 мегабайт.

В комплекте с концентратором поставляется USB-накопитель, содержащий образ системы в заводской конфигурации. Образ предназначен только для целей аварийного восстановления системы при недоступности иных способов. Образ создан с помощью комплекса «HDClone Pro» версии 3.9.

ВНИМАНИЕ!!! При восстановлении с заводского образа будут утеряны все данные, находящиеся на системном диске.

Аварийное восстановление осуществляется с помощью комплекса «HDClone», установленном на загрузочном USB-накопителе (накопитель не входит в комплект поставки, его требуется создать самостоятельно).

Необходимо подсоединить USB-накопители (загрузочный и с заводским образом) к свободным USB-портам концентратора и выполнить восстановление диска из образа. Общее описание работы комплекса можно найти на сайте производителя (http://www.miray.de/), далее в документе приведены особенности восстановления для концентратора «Дельта XP»:

— Перед включением концентратора подключить загрузочный USB-накопитель;
— При включении концентратора до появления окна загрузки Windows требуется нажать клавишу F11 на клавиатуре;
— Появится окно выбора устройства для загрузки системы (boot device). Требуется выбрать USB-накопитель (по умолчанию название начинается с USB);

— После загрузки «HDClone» подключить USB-накопитель с заводским образом;
— В появившемся окне «HDClone» следует выбрать копирование Image > Drive;
— В окне выбора исходного образа выбрать установленный USB-накопитель;
— Выбрать найденный образ системы;
— В окне выбора назначения при необходимости выбрать диск концентратора;
— Установка никаких дополнительных опций не требуется, следует продолжать восстановление стандартной навигацией по приложению «HDClone»;
— Убедиться, что после завершения выбора опций, нажатия кнопки Start и подтверждения операции началось копирование;
— Процесс копирования достаточно длительный и может занимать более получаса;
— После завершение копирования можно перезагрузить концентратор, удалить USB-накопители и начать работу в Windows.

4 УДАЛЕННОЕ АДМИНИСТРИРОВАНИЕ

Для удаленного администрирования используется комплекс «Remote Manipulator System». Описание комплекса можно найти на сайте производителя (http://rmansys.ru/). Далее в документы приведены некоторые особенности для концентратора «Дельта XP».

— Убедитесь, что концентратор запущен;
— На концентраторе предустановлена серверная часть комплекса, поэтому для администрирования требуется только установить на компьютер, находящийся в одной подсети с концентратором (в простейшем случае можно соединить компьютер и концентратор патч-кордом), клиентскую часть комплекса, которая называется «Remote Manipulator System Viewer». Скачать дистрибутив можно на сайте производителя, указанном выше;
— После установки программу следует запустить;
— Выбирается меню «Соединение»/«Добавить»;
— Указывается название соединения (на выбор пользователя) и IP-адрес концентратора. По умолчанию концентратору назначен адрес 192.168.0.1. Если настройка концентратора уже выполнялась, адрес может отличаться. Добавленное соединение появится в основном окне программы;
— Подключение выполняется двойным щелчком мыши по иконке соединения;
— В ходе соединения будет запрошен пароль, который задаётся в серверной части комплекса (на концентраторе). Пароль, установленный по умолчанию — «admin-root», без кавычек;
— После успешного соединения будет открыт рабочий стол концентратора — можно начинать работу. Если выполняется первое соединение, и возникают затруднения с входом в систему, обратите внимание на раздел 1 — начало работы.